

PLANT EEN BOOM.

JEROEN KNITEL

OVER DE EROSIE VAN PRIVACY ONLINE EN HET ZOEKEN NAAR CONTROLE

PRIVACY INSTELLINGEN
CONSISTENTIE VOORLICHTING
INTERNATIONALE AFSPRAKEN
KENNIS PROXY NEPPE INFORMATIE
GESLOTEN NETWERKEN
WETGEVING TRANSPARANTE SYSTEMEN
VPN FEEDBACK

PRIVACY CONTROLE



VOORNAAM
ACHTERNAAM

FAMILIELEDEN

GEBOORTEDATUM

FOTO-ALBUMS

MEDISCH DOSSIER

PARTNERS

CV

HOBBY'S

VRIENDEN

BANKGEGEVENS

KOOPGEDRAG

STRAFBLAD

POSTCODE

WOONPLAATS

JEROEN KNITEL 0444251

MA NIEUWE MEDIA EN DIGITALE CULTUUR
UNIVERSITEIT UTRECHT, 13 AUGUSTUS 2010

BEGELEIDER IMAR DE VRIES
TWEDE LEZER ERNA KOTKAMP

bedankt familie, vriendin, studiegenoten & begeleider*

*echte namen om privacy overwegingen niet genoemd.

inhoudsopgave

introdactie	4
privacy	7
1.1 toen was privacy heel gewoon?	7
1.2 vrijheid, blijheid: de waarde van privacy	8
1.3 informationele privacy	9
1.4 veiligheid versus commerciële belangen	11
1.5 operationeel in drie kaders	12
privacy & politiek	14
2.1 leren van reguleren	14
2.2 copyright kopie?	15
2.3 wetgeving in een flow van informatie	16
2.4 zoektocht naar grip, globale grip, benoembare grip	18
2.5 policy labyrint en zegels sparen	20
2.6 de politieke problemen	21
privacy & personen	23
3.1 euro's, dollars en info's	23
3.2 the presentation of self in everyday [Facebook] life	24
3.3 relaties & vertrouwen	25
3.4 voorkomen van schade, binnen alle contexten	27
3.5 publiek en privé	28
3.6 problemen op het sociale vlak	29
technologie	31
4.1 de ubiquitous paradox	31
4.2 jaren bewaren	32
4.3 toegang en beveiliging	34
4.4 overal en altijd	35
controle	37
5.1 beperking	37
5.2 convergentie	39
5.3 transparantie	40
5.4 (er)kennis	43
besluit	45
discussie	46
literatuur	47

introdunctie

Nog geen maand geleden stond ik in de verboden stad in Beijing, China. Een zee van donkerharige hoofden strekte zich uit over het grote plein voor me. Samen met mijn jongere broer en zus stond ik te luisteren naar onze gids totdat er een "excuse me, excuse me" klonk achter ons. Ik draaide me om en daar stond een Chinees meisje gewapend met een camera naar ons drietal omhoog te kijken: "Can I take picture with you, please?". Nog geen halve minuut later liep het meisje lachend met haar vriendinnen weg terwijl ze nog eens keken naar de verse foto op haar camera; een foto met drie lange blonde 'round eyes' en zichzelf. "Die zet ze op Facebook" grijnsde mijn broertje terwijl we ons weer omdraaiden naar de gids.

"Kleine kans dat iemand ons zal herkennen van haar Facebook-vrienden, toch?". Haar vrienden zullen ons inderdaad niet snel herkennen, maar hoe zit dat met Facebook zelf? In juli 2010 voegde de sociale netwerksite Facebook gezichtsherkenning toe voor een gedeelte van haar gebruikers: het systeem herkent gezichten op de geplaatste foto's en vraagt gebruikers de juiste persoon aan te geven bij het gezicht. Nu al, zijn gebruikers zonder dit hulpmiddel massaal foto's aan het 'taggen' waarin hun vrienden te zien zijn; profielen worden op deze manier gekoppeld aan gezichten op miljarden foto's. Het lijkt een kwestie van tijd totdat Facebook deze gigantische database aan gezichten behorend bij een profiel in gaat zetten voor het automatisch taggen van foto's. Twee jaar later krijgt het Chinese meisje van die bewuste dag in de verboden stad misschien wel een automatische notificatie van Facebook: "Jeroen Knitel is samen met jou gezien op een foto uit je album 'Beijing, 2010'. Wil je vrienden met deze persoon worden?".

Op deze manier krijgt de zin op de homepage van de sociale netwerksite: "Facebook helps you connect and share with the people in your life" toch een iets uitgebreidere interpretatie van "the people in your life". Maar er zijn nog veel meer mensen in je leven volgens sociale netwerksites (SNS) zoals Facebook. SNS helpen je namelijk ook met het verbinden met minder tastbare 'personen' in jouw leven in de vorm van adverteerders, onbekende applicatie ontwikkelaars en zakelijke partners van de SNS zelf (Nissenbaum, 2004 : 60). Wie deze mensen precies allemaal zijn is een onduidelijk gegeven, tot welke informatie zij toegang krijgen lijkt minder transparant te zijn dan de sites in de eerste instantie doen geloven; en wat er met deze informatie gebeurt is eveneens onduidelijk, zeker als er iets schort aan de beveiliging bij deze partners (Kincaid, 2010).

De disseminatie van persoonlijke informatie via online netwerken is een onderwerp dat met de voortdurende technologische ontwikkelingen en de groei die SNS als Facebook of services als die van Google doormaken de afgelopen paar jaar steeds vaker terug te vinden is in de verschillende media. Verlies en schending van privacy zijn sleutelwoorden in deze berichtgevingen. Het lijkt erop dat we de controle over onze privacy met de komst van het Internet en de daarop opererende diensten steeds meer verliezen, maar hebben we dat niet zelf in de hand?

Er ligt een zekere controle bij het individu waarbij men ervoor kan kiezen bijvoorbeeld niet op de foto te gaan met vreemden of geen account op Facebook te hebben. Maar waarom impliceert deze vorm van sociale participatie een verlies van privacy-controle? Dit hoeft geen logische oorzaak-gevolg relatie te zijn; informatietechnologie hoeft geen totaal verlies van privacy te betekenen. Het doel van dit onderzoek is om de verantwoordelijke processen te vinden die disseminatie van- en verlies van controle over privacy online bewerkstelligen en om uit deze processen oplossingen te distilleren op politiek, sociaal en technologisch vlak die ons helpen die controle weer terug te krijgen. Op deze manier kan zowel op maatschappelijk als wetenschappelijk vlak een bijdrage worden geleverd aan het privacy debat en haar stekeligheden. Dit onderzoek zal daarom draaien om het antwoord geven op de volgende vraag: "Op welke manieren kunnen verbeteringen worden aangebracht in het controleren en reguleren van individuele privacy online op sociaal, technologisch en politiek vlak?"

Om op bovengenoemde vraag een antwoord te kunnen geven moeten we deze fragmenteren tot concrete stappen die ons leiden tot het uiteindelijke antwoord. Van filosofie tot mediawetenschap, sociale, politieke en juridische theorieën en (informatie)technologie; het theoretische landschap van het concept privacy is druk bevolkt. Het is daarom van belang dat een werkbare conceptualisatie van privacy wordt gevormd waarin het informationele aspect benadrukt wordt en de relevante actoren worden beschreven. Het eerste hoofdstuk biedt hier ruimte voor en door middel van Daniel Solove zijn werk in "A Taxonomy of Privacy" (2004) en de bijdrage van Helen Nissenbaum (2009) schets ik een concept waarmee in dit onderzoek gewerkt kan worden.

In de drie hoofdstukken die volgen na de conceptualisatie zal in het politieke, sociale en technologische kader achtereenvolgens door middel van een discours-analyse en relevante voorbeelden uit de praktijk de problemen met betrekking tot privacy online worden beschreven. In de zoektocht naar verbeteringen moet er namelijk, om tot een definiëring van deze verbeteringen te komen, eerst gekeken worden welke problemen precies spelen en hoe zij tot stand komen.

Op het politieke vlak zijn vooral problemen te vinden in het ontbreken van convergentie in regulering en de kennis van niet alleen privacy zelf maar ook de technologie die er afbreuk aan doet. Op sociaal vlak speelt identiteitsvorming, relaties en wederom het onbekend zijn met de exacte complicaties die gepaard gaan met het delen van informatie een rol. Als derde wordt duidelijk dat op technologisch vlak de groeiende mogelijkheden tot dataverzameling en -opslag en de complicaties met betrekking tot de beveiliging en toegang daarvan ook hun aandeel hebben in het verlies van controle.

Door het blootleggen van deze problemen worden ze tastbaarder en begrijpelijker waardoor het komen met oplossingen ook makkelijker wordt. Door het benoemen van kernbegrippen waarin we ruimte voor verbetering moeten zoeken, zet ik in het vijfde hoofdstuk over controle de mogelijkheden uiteen die we op de verschillende vlakken, en in een hybride van deze, hebben om de controle over privacy online weer terug te winnen. Op deze manier kan een begrip van de huidige situatie op politiek, sociaal en technologisch vlak en voor iedere actor hierin leiden tot het vinden van concrete oplossingen.

De titel van dit stuk is “plant een boom” die de uiteindelijke oplossingen om de erosie van privacy online tegen te gaan onderstreept; bomen geven grip op de eroderende grond, het planten van bomen suggereert een teruggroei van controle. De zoektocht naar deze controle staat centraal in dit onderzoek, de oplossing ervoor lijkt zoals het planten van een boom simpel: doe niet zomaar afstand van je persoonlijke informatie. Dat dit in beide gevallen complexer is dan het lijkt zal duidelijk worden gaandeweg de zoektocht zich verder ontwikkelt. De verschillende kaders waarin problemen opspelen en de conflicterende belangen hierin zorgen voor een netwerk van actoren dat duidelijk maakt waarom de oplossing niet te zoeken is in enkel het planten van een boom maar een combinatie van verschillende factoren die samen privacy kunnen vasthouden zonder dat het onder onze voeten wegglijdt.

privacy

Om voor dit onderzoek een werkbaar concept van privacy te hebben is het nodig om dat hier allereerst uiteen te zetten. Het conceptualiseren van privacy is op zichzelf al een compleet wetenschappelijk debat te noemen. De enige collectieve overeenstemming die te vinden is in dit debat lijkt ook de meest onbevredigende: privacy is een complex en verwarrend onderwerp om te conceptualiseren: “privacy means so many different things to so many different people that it has lost any precise legal connotation that it might once have had” (McCarthy in Solove 2006 : 479). Maar had privacy dan ooit wel één algemeen aangenomen connotatie zoals hier wordt geïmpliceerd? Om hier achter te komen moet er een stap terug in de tijd worden genomen en een blik op de historie van privacy worden geworpen.

1.1 toen was privacy heel gewoon?

De beginjaren van privacy zijn volgens enkelen al te vinden in religieuze werken als de Koran en de Bijbel (Hixson, 1987) maar voor een eerste gedefinieerde legale connotatie van privacy moeten we naar het Groot Brittannië van de 14e eeuw. In 1361 werd daar bij de Justices of Peace Act al besloten tot het arresteren van gluurders en afluisteraars (Michael, 1994). Men had het recht op zijn eigen persoonlijke domein zonder dat anderen daar ongewenst in meedeelden. Dit idee werd later in de 18e eeuw nog verder gegoten in een vorm van zogenoemde ‘territoriale privacy’ (Langheinrich, 2001) door de eveneens Engelse parlementariër William Pitt: “The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow though it; the storms may enter; the rain may enter – but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement” (Pitt in Langheinrich, 2001 : 274). Anders gezegd, mensen moeten een plek kunnen hebben waar ze alleen kunnen zijn.

Dit is ook het grondbeginsel uit een van de meest geciteerde werken rondom ‘het begin’ van privacy van Samuel Warren en Louis Brandeis “The Right to Privacy” (1890). Hierin wordt privacy vooral ‘het recht om alleen gelaten te worden’ genoemd. Dat recht wordt vervolgens voornamelijk gebruikt om een ‘uitweg’ te hebben bij de technologische ontwikkeling van de fotografie en de drukpers; het ongevraagd op de foto zetten van personen en het verspreiden van deze foto’s werd namelijk een stuk meer laagdrempelig door deze technologieën.

De notie van het recht op een persoonlijk domein door de Justices of Peace Act kan ook aan een ander aspect van privacy worden toegekend, dat van communicatie. Volgens John Durham Peters (1999) in zijn *Speaking into the Air* geeft de komst van de enveloppe in 1849 de brief een compleet nieuwe atmosfeer van privacy (idem : 166). Deze nieuwe atmosfeer ligt deels besloten in de privacy van communicatie, een die met de komst van de technologische ontwikkelingen vanaf de 19e

eeuw, zoals de telefoon, een grote ontwikkeling doormaakte met een uiteindelijke Electronic Communications Privacy Act in 1986 tot gevolg.

Deze nieuwe atmosfeer ligt dus deels besloten in de privacy omtrent communicatie maar kent ook een tweede, voor dit onderzoek vooral belangrijk, aspect: dat van privacy van informatie, ook wel *informationele privacy* genoemd. Een aspect van privacy dat wellicht deels is begonnen bij de enveloppe maar rond 1960-1970 met het toegenomen gebruik van elektronische dataverwerking een hoge prioriteit heeft gekregen op politiek, sociaal en technologisch vlak.

Privacy gedefinieerd als 'het recht om alleen gelaten te worden' wordt hierdoor aangevuld met '*het recht om te kiezen welke informatie over jou beschikbaar is voor wie*'; een aspect van privacy waar wij als individu het liefst controle over willen hebben maar waar het, wat duidelijk wordt in dit werk, vooral op de verantwoordelijkheid van derde partijen aankomt als het gaat om de opslag dan wel vrijgeven van deze informatie. In de volgende paragraaf illustreer ik dit ongewild vrijgeven van informatie als belangrijke beweegreden om te pleiten voor privacy aan de hand van een voorbeeld. Hiermee wordt ook de intrinsieke waarde van privacy, de manier waarop het de mogelijkheid impliceert om deze als individu te kunnen controleren en de gevolgen van het verliezen ervan duidelijk gemaakt.

1.2 vrijheid, blijheid: de waarde van privacy

"Privacy is an especially important and good thing for human beings" (Reiman, 1995: 33), privacy is belangrijk, waardevol en moet gewaarborgd blijven. Maar, waarom eigenlijk? Waarin de waarde van privacy vooral terug te vinden is, is de mate van vrijheid die het impliceert (o.a. Gavison, 1980; Reiman, 1995).

Om het belang van vrijheid en daarmee privacy aan te tonen stelt Jeffrey Reiman (1995) een gedachte-experiment voor dat een 'informational panopticon' beschrijft. Het idee van het panopticon, het eerst beschreven door de Engelse filosoof Jeremy Bentham (Bennett, 1995), houdt een gevangenis in waarbij een observant alle gevangenen in de gaten kan houden zonder dat de gevangene weet wanneer hij/zij in de gaten wordt gehouden. Dit heeft tot gevolg dat een gevangene zijn gedrag aanpast aan het feit dat hij of zij constant in de gaten gehouden kan worden zonder dat dit zo hoeft te zijn. Reiman (1995) en iets minder concreet Gavison (1980) gebruiken het panopticon om de waarde van privacy aan te tonen.

Want, zo beargumenteert Gavison, mensen hebben een zekere 'ademruimte' nodig om te kunnen experimenteren in de dingen die ze doen zonder constant afgeleid te zijn door het feit dat ze weleens in de gaten zouden kunnen worden gehouden en bang moeten zijn voor afkeuring, censuur of voor ridicularisatie. Dit gebeurt wanneer een individu al zijn handelingen in het perspectief van een derde persoon gaat zien, wat spontaniteit en vrijheid in handelen tegen zou gaan. Privacy kan daarom gezien worden als een oplossing voor deze 'remming' in zelfontplooiing en uiting: omdat privacy

functioneert "as a means of protecting freedom, moral personality, and a rich and critical inner life" (Reiman, 1995 : 42). Privacy beslaat hiermee ook *self-ownership* en individuele soevereiniteit.

De parallel met het panopticon kan verder worden getrokken in het huidige landschap rondom informatieve privacy en informatietechnologie; namelijk het centrale punt waarbinnen iedereen gezien kan worden in de gevangenis. Met de opkomst van centrale databanken waarin de persoonlijke informatie van grote groepen mensen opgeslagen worden, wordt het mogelijk deze vanuit centrale punten te benaderen en op te vragen (Nissenbaum, 2009 : 75). Wat deze persoonlijke informatie precies inhoudt en welke processen hierin spelen is de volgende stap naar een concrete conceptualisatie van privacy, informatieve privacy.

1.3 informatieve privacy

Van de verschillende aspecten van privacy wordt in dit onderzoek gewerkt met het informatieve aspect van privacy: privacy van informatie. De persoonlijke informatie waar het daarbij om gaat betekent in dit onderzoek alle informatie die aan een te identificeren of geïdentificeerde natuurlijke persoon ('data subject') is gerelateerd. Een identificeerbaar persoon is iemand die kan worden geïdentificeerd, direct of indirect, door een identificatienummer of andere factoren die specifiek zijn voor zijn of haar fysieke, psychologische, geestelijke, economische, culturele of sociale identiteit.¹

In deze flow van persoonlijke informatie is het van belang om te kijken naar de verschillende processen die hierin een rol spelen. Daniel Solove brengt met zijn artikel "A Taxonomy of Privacy" (2006) een duidelijke classificatie in kaart van de processen en entiteiten die een rol spelen rondom deze privacy van informatie. Omdat Solove hierin vooral op zoek is naar de relevantie voor regulering en wettelijke veroordeling kijkt hij nadrukkelijk op welke manier activiteiten rondom informatieve privacy-problemen kunnen veroorzaken voor zowel het individu als maatschappij (idem : 485).

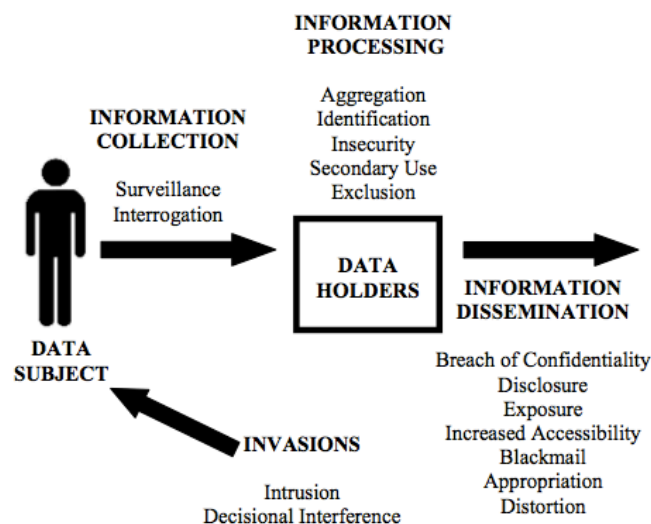
De taxonomie die Solove schetst kent vier groepen: *information collection*, *information processing*, *information dissemination* en *invasion*. Deze groepen zijn gecentreerd rond de informatie van een individu waaromheen entiteiten als het publiek, bedrijven en de overheid deze respectievelijk verzamelen, opslaan en verwerken, verspreiden of 'invasies plegen' ofwel inbreuk maken op de directe persoon zijn/haar privacy (afbeelding 1). Solove laat zien dat niet alleen de technologie maar ook de actoren zoals mensen, bedrijven en de overheid de oorzaak zijn van deze problemen.

Van deze vier probleemgebieden wordt de laatste, *invasion*, voor dit onderzoek bewust achterwege gelaten omdat niet geheel duidelijk is wat Solove met dit probleemgebied precies wil beschrijven op het gebied van informatieve privacy. De aandacht ligt bij dit probleemgebied op het binnendringen van iemands privé omgeving en de tussenkomst van derden bij het maken van persoonlijke beslissingen. Dit zijn zaken die niet direct expliciet met informatieve privacy te maken hebben en blijven daarom dus achterwege in dit onderzoek. De overige drie probleemgebieden zijn

¹ Voor een volledige definitie van "personal information" zie de European Union Directive hoofdstuk 1, artikel 2

wel bruikbaar voor dit onderzoek omdat zij de stappen in de flow van informatie duidelijk beschrijven en daarmee werkbare 'gradaties' opleveren in het informatieproces. Hieronder behandel ik kort deze drie onderdelen om de processen en daarin besloten probleemgebieden rondom informatiele privacy bloot te kunnen leggen en aan te vullen.

Zonder informatie zijn er geen problemen met informatie. Daarom begint Solove logischerwijs met deze eerste stap in de taxonomie van informatiele privacy; het verkrijgen van informatie: information collection. Deze kent twee subcategorieën van problemen: *surveillance* en *interrogation*. Wat ontbreekt bij information collection is nog een belangrijke derde subcategorie. Want hoewel Solove de nadruk legt op privacy-problemen in zijn framework lijkt het (vrijwillig) afdragen van informatie door een persoon niet een probleem te zijn dat hij noemt. Een belangrijk argument wat ik wil maken in dit stuk is waarom juist deze manier wél problematisch is in het huidige tijdperk van onze informatiemaatschappij. Hierin ligt namelijk de oorzaak voor een verdere verspreiding of erosie van deze informatiele privacy.



afbeelding 1: Soloves processen rondom informatiele privacy (Solove, 2006 : 490)

De verdere erosie vindt dan vooral plaats bij de volgende categorieën information processing en de daaropvolgende information dissemination die de problematische actoren inhouden rondom het eroderen van deze informatiele privacy. Wanneer persoonlijke informatie vloeit naar een instantie door middel van het vrijwillig afgeven van deze informatie, hoe weet men dan of deze informatie veilig is? Wordt deze beveiligd opgeslagen? Wie hebben er binnen (of zelfs buiten) deze instantie toegang tot die informatie? Transparantie bij het verzamelen van persoonlijke informatie is een belangrijk aspect dat ik in de komende hoofdstukken nog verder uit zal werken. Voor nu is het belangrijk om de problemen in de gevolgen van deze drie vormen van information collection te zien in de verwerking en verspreiding van informatie.

Met een duidelijk zicht op de processen binnen informatieve privacy en de daarmee gepaarde problemen is er weer een stap dichterbij gezet naar een werkbare conceptualisatie van privacy voor dit onderzoek. Deze conceptualisatie in zijn huidige vorm kent een breed speelveld waarin twee actoren voornamelijk aanwezig zijn: de overheid en de commercie. Omdat deze actoren op verschillende uiteenlopende manieren deelnemen aan het privacy debat is het belangrijk een van deze te kiezen en mee te werken om tot een grondige en bruikbare analyse te kunnen komen voor dit onderzoek.

1.4 veiligheid versus commerciële belangen

Dat de opkomst van de informatietechnologie als bedreiging wordt gezien voor individuele privacy lijkt een algehele consensus te zijn in het debat rondom technologie en privacy in het algemeen. Onder andere Philip Agre en Marc Rotenberg tonen met hun boek *Technology and Privacy: The New Landscape* (1997), aan dat het landschap rondom privacy met de komst van (informatie)technologie drastisch veranderd is. In de verschillende werken uit dit boek zijn grofweg twee actoren aan te wijzen die persoonlijke informatie verzamelen binnen deze wisselwerking tussen informatietechnologie en privacy.

Allereerst is de regerende instantie aan te wijzen als belangrijke actor. 'De overheid' zoals er vaak naar wordt verwezen is hierbij de regering van een land dat verantwoordelijk is voor het algeheel functioneren van de maatschappij. Een belangrijke verantwoordelijkheid in het takenpakket van de overheid is het waarborgen van de 'veiligheid'. Het is vaak in het belang van deze taak dat de privacy van het individu onder druk komt te staan (Whitaker, 1998). Toezicht op het publiek door middel van *closed-circuit television* (CCTV), dat vooral op grote schaal wordt gebruikt in Groot-Brittannië, of door middel van het opslaan in databanken van persoonlijke informatie en het koppelen ervan (Flaherty, 1988) zijn twee van de middelen die veel negatieve kritiek te verwerken krijgen.

Schrijver George Orwell waarschuwde met zijn boek *Nineteen Eighty-Four* (1949) in 1949 al voor een overheid die ons, als individu, volledig in de gaten zou houden en waar mogelijk onze keuzes beïnvloeden door middel van toezicht, misinformatie en bureaucratie. Deze door Orwell geschetste dystopie is tot op de dag van vandaag geen werkelijkheid geworden maar heeft wel een zekere bewustwording gecreëerd voor het grote publiek (Lessig, 2006: 209). Eenzelfde mate van bewustwording wordt tegenwoordig gecreëerd met alle media-aandacht die er is voor de tweede actor binnen het verzamelen van persoonlijke informatie.

Deze tweede actor kunnen we zien in de instanties die niet opereren vanuit politieke overtuigingen in opdracht van de regering, maar de instanties, bedrijven, personen die handelen vanuit ander oogpunt; vooral het commerciële belang weegt hier zwaar (Samarajiva, 1997). Het huidige economische klimaat groeit meer en meer naar een 'customized' model waarbij bedrijven zich niet meer richten op de massa maar juist op het koopgedrag en behoeftes van de individuele consument. Dit is toe te schrijven aan de voortdurende technische ontwikkelingen die dit mogelijk

maken in tegenstelling tot de vroegere commerciële domeinen. Informatietechnologie en flexibele productie staan aan de vooravond van deze gerichte verkooptechnieken en de mogelijkheden om deze zo efficiënt mogelijk aan te bieden blijven zich uitbreiden (idem).

Dit onderzoek zal zich richten op de bedrijven-sector als actor binnen het verzamelen van persoonlijke informatie en niet op de overheid en het veiligheidsaspect om een tweetal redenen. Allereerst zijn de commerciële belangen waarmee de bedrijven sector deze persoonlijke informatie verzamelt, opslaat en gebruikt op moreel vlak meer verwerpelijk dan wanneer de overheid diezelfde of andere persoonlijke informatie gebruikt ten behoeve van een algemeen belang: de collectieve veiligheid. Daarnaast staat het gebruik van de diensten uit deze bedrijven sector dichterbij de meeste individuen in termen van persoonlijke levenssfeer en de gevolgen ervan (Nissenbaum, 2009) dan die van bijvoorbeeld het verstrekken van de vingerafdruk voor het paspoort of het volgen van het reisgedrag bij het gebruik van de OV chip kaart (OV-Chipkaart, 2010). Het is om deze redenen dat ik voor dit onderzoek vooral in zal gaan op de bedrijven-sector en haar functioneren op het gebied van informatiele privacy en ruimte voor de overheid als actor bij informatiele privacy-processen aan andere academici overlaat.

1.5 operationeel in drie kaders

In het debat rondom de conceptualisatie van privacy is er een polarisatie te zien tussen het definiëren van privacy vanuit normatieve en operationele argumenten (Bellotti, 1997 : 66). De normatieve definitie van privacy beslaat vooral de notie dat bepaalde aspecten van het individu en zijn/haar activiteiten privé zijn en niet kenbaar gemaakt mogen worden: "Privacy is the condition in which others are deprived of access to you and in order for there to be a right to privacy there must be some valid form specifying that some personal information about or experience of individuals should be kept out of other individuals' reach" (Reiman in Bellotti, 1997 : 66). Dit is alleen geen werkbare definitie voor dit onderzoek aangezien het niet universeel is voor iedereen. Context speelt een grote rol. Waar gebeurt het? Met wie? Het is moeilijk om te beslissen wie wanneer en waar toegang heeft tot wat en in welke context. Deze variabiliteit zorgt ervoor dat we geen collectief perceptueel concept hebben om mee te werken.

We kunnen een dergelijk concept wel vinden in de operationele definitie van privacy die refereert naar "de mogelijkheid om". Bijvoorbeeld *access control*: de mogelijkheid om controle te hebben over je eigen persoonlijke informatie. Samarajiva (1997) noemt dit de "control of outflow of information that may be strategic or aesthetic value to the person and the control of inflow of information" (idem : 283). Een operationele definitie is ook praktischer voor het ontwerpen van systemen die met persoonlijke informatie te maken hebben en in het geval van dit onderzoek voor het bieden van oplossingen voor het behouden van controle over deze voor het individu.

Deze controle over toegang tot de out- en inflow van persoonlijke informatie is het type definitie dat we zoeken in het operationele veld waar de problemen bij "de mogelijkheid om controle te

hebben over persoonlijke informatie” spelen. Dit veld is uit te zetten over drie verschillende kaders die controle kunnen bieden. Deze zijn te vinden in politieke regulering, sociale normen en de technologie (o.a. Agre en Rotenberg, 1997; Lessig, 2006; Nissenbaum, 2010). In de komende drie hoofdstukken behandel ik de problemen ten aanzien van privacy online die in deze kaders de kop op steken, te beginnen met het politieke kader.

privacy & politiek

Met de komst en ontwikkelingen op het gebied van informatietechnologie heeft het politieke landschap van privacy een aardige aardbeving te verwerken gehad die eigenlijk nog steeds voortduurt. De Europese overheden en gezamenlijke commissies hadden het moeilijk met de snelle opkomst van de computer- en informatietechnologie in het begin van de jaren '70. Dit toen relatief nieuwe medium riep veel vragen op en was verantwoordelijk voor een groeiend aantal onzekerheden. Om deze vragen- en onzekerheden deels te beantwoorden zocht men de basis voor een wet dat deze nieuwe ontwikkelingen omsloot (Davies, 1997). Tot op de dag van vandaag is men nog steeds op zoek naar een dergelijke ultieme wettelijke regulering. Het lijkt erop dat met de ontwikkelingen en innovatie in mogelijkheden voor het verzamelen, verwerken en opvragen van informatie, die in een constante staat van flux verkeren, ook het juridische veld rondom informationele privacy zich hierdoor in een flux bevindt. Het begrijpen van deze flux van regulering en de problemen die hierin spelen is het doel van dit hoofdstuk. Om te beginnen is het van belang weer een werkbaar concept te hebben voor de rest van het hoofdstuk, dit keer van regulering.

2.1 leren van reguleren

De hoofdvraag in dit onderzoek stelt “controleren en reguleren” als twee verschillende zaken. Per definitie is dit ook zo; reguleren is een vorm van controleren: “control or supervise [...] by means of rules and regulations”.² Letterlijk vertaald is reguleren het controleren met het gebruik van ‘regels’ en ‘statuten’. Het verschil tussen regels en statuten kan worden betwist maar is voor dit punt van onderzoek niet belangrijk, wat wel belangrijk is, is vanwaar deze regels worden opgelegd. Wie bepaalt deze regels? Zijn dit wettelijke bepalingen of zijn de verantwoordelijke partijen in de opstelling van deze regels verder te zoeken dan alleen bij de overheid? Lawrence Lessig stelt in zijn boek *Code 2.0* (2006) dat er wel zeker meerdere actoren zijn aan te wijzen in de manier waarop gereguleerd wordt.

Regulering vindt namelijk niet alleen plaats door wettelijke bepalingen maar ook door nog drie andere actoren die alledrie hun eigen invloed hebben op het te reguleren object: de markt, de (sociale) normen en de architectuur of technologie (idem). Voor het Internet betekent dit dat de markt kan reguleren op het gebied van het bepalen van de prijs voor internettoegang of andere online services. De normen die gelden in verschillende online gemeenschappen zorgen voor het in stand houden ervan. Tot slot zorgt de architectuur van bijvoorbeeld een Virtual Private Network (VPN) ervoor dat alleen een selecte groep mensen toegang heeft tot bepaalde diensten.

Toch kan ‘de wet’ een grotere rol spelen dan de overige drie actoren bij regulering al moet het er wel ten alle tijden rekening mee houden. Wetgeving heeft de mogelijkheid om zowel direct als indirect te reguleren op de drie andere actoren, maar het opstellen van een dergelijke wet op het

² Definitie afkomstig uit Dictionary: Apple Inc. (2010)

Internet is een constante zoektocht naar een 'equilibrium': "requiring consideration of not only [...] legal adjustments, but also predicting the responsive effects such changes will stimulate" (Wagner in Lessig, 2006 : 130). Voor dit hoofdstuk is het daarom belangrijk te kijken op welke manier deze politieke regulering van wetten direct danwel indirect zijn weerslag vindt op zichzelf en de andere actoren en in hoeverre dit problemen oplevert voor het controleren en reguleren van informationele privacy. Om deze in te leiden kijk ik eerst naar een actueel voorbeeld dat veel overeenkomsten vertoont met het privacy debat online; dat van copyright.

2.2 copyright kopie?

De problemen van privacy en copyright zijn in het kader van de ontwikkelingen van informatietechnologie bijna exact hetzelfde; er is een gedeelte van 'onze' informatie waar 'we' de controle over hebben verloren. In het geval van copyright is het de data die een kopie van het auteursrechtelijk beschermde materiaal bevat; bij privacy is het de data die feitelijke informatie over een persoon bevat. In beide gevallen is het Internet er voor verantwoordelijk dat we de controle zijn verloren: copyright omdat het Internet ervoor zorgde dat er gratis kopieën gemaakt en verspreid konden worden, en privacy bijvoorbeeld omdat de technologie een constante en goedkope monitoring van ons gedrag kan bewerkstelligen.

Maar er zijn ook verschillen tussen beide probleemgebieden, deze zijn te vinden in de politieke economie; vooral de belangenverstrengelingen zijn verantwoordelijk voor een onevenwichtige aanpak van de problemen. In het geval van copyright zijn de partijen die pleiten voor een duidelijke copyright regulatie en daarmee de belangen die bedreigd worden duidelijk en georganiseerd; filmdistributeurs, muzikanten, instanties als de RIAA in de Verenigde Staten en bijvoorbeeld Stichting BREIN in Nederland vechten tegen alle mogelijke partijen die inbreuk maken op het auteursrecht op Internet. In het geval van privacy zijn de belangen die bedreigd worden meer diffuus en ongeorganiseerd. Veiligheid en bedrijfsefficiency zijn argumenten voor de afbrokkeling van privacy van partijen als de overheid en de commerciële sector (Samarajiva, 1997), daartegenover staan de consument en instanties als Bits of Freedom die vechten voor het behoud van individuele privacy op internet. Het resultaat van deze strijdige belangen heeft de wettelijke regulering aanzienlijk vertraagd voor informationele privacy: "The result of these differences, as any political theorist would then predict, is that over the past ten years, while we've seen a lot of legislative and technical changes to solve the problems facing copyright, we've seen very few that would solve the problems of privacy" (idem : 216).

De basis voor deze wet zou leunen op de principes die ik in het eerste hoofdstuk heb genoemd; het verzamelen, verwerken en distribueren van persoonlijke informatie. Deze processen moeten vervolgens op grond van een eerlijke en precieze manier in samenspraak met, of met goedkeuring van gebruikers van informatie in de privé en publieke sectoren worden beschreven in die wetten. In theorie klinkt dit als een solide constructie voor bescherming van de persoonlijke informatie,

in de realiteit worden deze principes en de instanties aangewezen voor het reguleren hiervan verantwoordelijk gehouden voor de beperkte invloed die ze uiteindelijk op deze processen uitoefenen. De grootste tekortkomingen in deze wettelijke bepalingen zijn vaak dat het geen daadwerkelijke privacy-wetten zijn maar meer informationele wetten (Davies, 1997 : 157).

Dat het er weinig zijn wil niet zeggen dat de regulering omtrent privacy om de strijdende belangen geen aandacht geniet. Net zoals er pogingen worden gedaan bij copyright kan ook de balans bij het beschermen van privacy hersteld worden. We moeten hiervoor op zoek naar een kruisbestuiving van wetten, normen, markt en technologie die de geschikte vorm van controle realiseert en een veilige online privé omgeving kan herstellen. Om dit te kunnen realiseren moeten eerst de problemen in het politieke kader van informationele privacy bloot worden gelegd om vervolgens deze in de andere twee kaders te benoemen en de uiteindelijke kruisbestuiving invulling te kunnen geven.

2.3 wetgeving in een flow van informatie

Een van de problemen waarmee een politieke regulering van privacy dus te kampen heeft is de belangenstrijd tussen de commerciële sector en het individu zelf (al dan niet gerepresenteerd door instanties zoals BoF). Het technologisch deterministische uitgangspunt van een voortdurende ontwikkeling van informatietechnologie wordt gezien als belangrijke verantwoordelijke voor een moeizaam pakket van wettelijke bepalingen rondom de flow van persoonlijke informatie.

Simon Davies (1997) betoogt dat het probleem met de wetgeving in Europa en de Verenigde staten rondom databescherming en privacybescherming eigenlijk is dat het allemaal neerkomt op enkel databescherming: "[T]hey are seldom privacy laws. They are information laws protecting data before people [...] they deal only with the way personal data is collected, stored, used and accessed" (1997: 156). Zijn grootste punt van kritiek is dat deze wetten weinig uithalen voor het voorkomen of beperken van het verzamelen van informatie.

Ik zie, in tegenstelling tot Davies, geen problemen in het gebruik van de wetten rondom databescherming voor het reguleren en beschermen van privacy. Immers, alle aspecten die hun invloed uitoefenen op de privacy van een individu zijn hierin opgenomen. Dat deze wetten rondom databescherming incompleet zijn in hun huidige vorm is wel een valide punt van kritiek. De oorzaak van deze onvolledigheid is te zoeken in een voortdurende strijd tussen technologie en toepasbare regelgeving op deze technologie. Een strijd die al sinds de begindagen van de informatietechnologie voortduurt:

David Flaherty zei al in 1988 wat tot op de dag van vandaag nog van toepassing is: "there is a real risk that data protection of today will be looked back on as a rather quaint, failed effort to cope with an overpowering technological tide" (Flaherty, 1988 : 384). Ook nu zijn onze huidige wetten, zij het in Nederland, Europa of de Verenigde Staten ontoereikend om een wettelijke leidraad te bieden aan de meest intelligente manieren om informatie te verzamelen, te verwerken en toegang tot te

verlenen. Men loopt achter de technologie aan als het gaat om de wetgeving rondom databescherming en daarmee privacy online.

Reinventing Data Protection? van Serge Gutwirth et al. (2009) is het bewijs van de trage wetgeving en strubbelingen die gepaard gaan met de alsmaar voortdurende ontwikkelingen op het gebied van informatietechnologie; het is een uitgebalanceerd werk over het huidige debat rondom databescherming en privacy. De werken hierin gaan allen in op de huidige Europese wetgeving van databescherming en zetten deze af tegen de introductie van "increasingly powerful, miniaturized, ubiquitous and autonomic forms of computing" (Gutwirth et al. 2009: 7).

De flexibiliteit en snelheid waarmee technologie zich ontwikkelt, kent de wetgeving helaas niet. Dat nieuwe wetten niet met dezelfde snelheid ingevoerd kunnen worden als dat de technologische middelen zich uitbreiden en verder ontwikkelen is, gezien de implementatieprocedure, een feit. De tijd voor het implementeren van een nieuwe wet in Nederland overschrijdt al gauw dat van een jaar.³ De technologie lijkt alles behalve 'haasje over' met de wettelijke regulering te spelen; het is een oneerlijke race op een circuit waarbij de technologie talloze keren voorbij komt sprinten als het aan het zoveelste rondje begint dat het verder van de wettelijke regulering uitloopt. Deze achterstand komt door de genoemde oorzaken maar ook door het volgende nieuwe begrip.

Erkennis, het is een woord dat we in het Nederlands niet kennen maar waarvan ik zou willen zeggen dat het een deel van de privacy-problemen online en het aanpakken hiervan in de politiek perfect beschrijft. Er is namelijk een causaal verband aan te tonen tussen het gebrek aan kennis over het informationele privacy-probleem in combinatie met de huidige (en komende) mogelijkheden binnen de informatietechnologie wat daarmee tegelijkertijd een gebrek aan het erkennen van de huidige (en komende) problemen van informationele privacy online inhoudt. In *Privacyregulering in theorie en praktijk* van J. Berkvens en C. Prins (2007) schrijft J. Terstegge dat we ons bevinden in een nieuwe wereld met oude privacy-beginselen. Dat dit dé oorzaak is van de tot nu toe falende politieke regulering van informationele privacy online is, kunnen we niet zo zeggen. Dat dit één van de oorzaken is wel. Een andere oorzaak is bijvoorbeeld de achter de feiten aanhobbende overheden: "The public is being lulled into a false sense of security about the protection of their privacy by their official protectors, who often lack the will and energy to resist successfully the diverse initiatives of what Jan Freese (one of Europe's first data-protection commissioners) has aptly termed the 'information athletes' in our respective societies" (Davies, 1997 : 157). Maar zelfs als de overheid wél een consistente en duidelijke kennis van het probleemgebied heeft, hoe kan daar vervolgens op geanticipeerd worden? De volgende paragraaf belicht de problemen en mogelijkheden in het vormen en naleven van deze wetten en hun terrein van jurisdictie.

³ Zie "Implementatieprocedure via formele wetgeving" <<http://www.montesquieu-instituut.nl/9353000/1/j9vvhfxcd6p0lcl/vha1jzotbmpc>>

2.4 zoektocht naar grip, globale grip, benoembare grip

De eerdergenoemde parallel met copyright blijft ook in het volgende probleem bij het reguleren van informatiele privacy online intact; het probleem dat besloten ligt in het medium zelf, het Internet. De grenzeloosheid van het medium geeft problemen met betrekking tot het naleven van nationale wettelijke bepalingen. Lessig noemt het voorbeeld van iCrave TV: een Canadese website die, volgens Canadese wetten, volledig legaal televisie-series uitzond via het Internet. Het was immers volgens de Canadese wet legaal om de reikwijdte van een televisie-uitzending, zolang deze onaangepast was, te vergroten (Lessig, 2006 : 295). Dit stootte tegen de borst van Amerikaanse content-aanbieders die zich direct beklagden bij iCrave TV. Het uitzenden van televisie-uitzendingen via Internet was in de Verenigde Staten namelijk wél aan een stelsel van wetten en vergoedingen verbonden en laat het Internet nu ook gewoon toegankelijk zijn in de Verenigde Staten. Middels verschillende rechtszaken werd iCrave TV gesommeerd om Amerikaanse bezoekers te weren van haar website, een eis die technisch gezien nooit volledig te realiseren is.

Technisch, maar ook conceptueel vormt het een probleem, want wanneer men achter de computer zit en zich op het Internet bevindt, bevinden we ons dan in de ‘anarchie’ van het Internet of gewoon ‘achter de computer’ in ons eigen land? Welke ruimte is verantwoordelijk en in welke ruimte moeten we dan de jurisdictie zoeken? Het antwoord is: allebei. Het probleem voor ‘de wet’ is om uit te zoeken welke normen in deze twee gebieden gelden en hoe deze nageleefd moeten worden in welke context op het Internet. Dit probleem alleen al geeft ruimte voor een academisch debat wat ik hieronder wil schetsen en vervolgens op wil reflecteren. Er zijn kort gezegd drie ‘kampen’ binnen dit debat; een kamp dat pleit voor een totaal nieuwe vorm van regulering, een tweede die gebaseerd is op bestaande internationale regulering en een laatste kamp dat het Internet in landelijke zones wil verdelen.

Allereerst het kamp van David Post en David Johnson (1996): “The rise of an electronic medium that disregards geographical boundaries throws the law into disarray by creating entirely new phenomena that need to become the subject of clear legal rules but that cannot be governed, satisfactorily, by any current territorially based sovereign” (idem : 1368). Cyberspace is ‘ergens anders’, en dat ‘ergens anders’ moet zijn eigen regelgeving krijgen. Online gedrag kan niet gereguleerd worden vanuit bestaande gebieden. Of zoals Milan Kundera zegt: leven in cyberspace is een leven ergens anders (Kundera in Lessig, 2006 : 301).

Dan zijn er Jack Goldsmith en Tim Wu (Goldsmith en Wu, 2006) die zeggen dat het jurisdictieprobleem dat nu opspeelt met het Internet niets nieuws is. Grensoverschrijdende incidenten die betrekking hadden op internationale wetgevingen zijn er altijd geweest. De wet heeft altijd gewerkt voor deze conflicten van autoriteit. Het Internet mag dan wel het aantal van deze conflicten doen verhogen, het verandert niet de eigenschappen. Oude structuren moeten misschien gegoten worden in deze nieuwe vorm, maar het oude patroon zelf zal overleven.

Lawrence Lessig geeft beide partijen deels gelijk maar komt zelf met een vooral rigoureuze technologische oplossing. Het is volgens Lessig zaak het Internet in zone's te verdelen die de kwalificaties van iedere individuele gebruiker respecteert. Zo wordt iedere gebruiker gereguleerd vanuit de in zijn land geldende wetten en regels (Lessig, 2006 : 309).

Post en Johnson hebben gelijk in het feit dat er iets 'nieuws' is, maar niet een nieuwe soort van jurisdictie, hooguit een nieuwe gradatie hierin. Goldsmith en Wu zien terecht overeenkomsten met de eerder altijd voldoende internationale rechtspraak maar missen de nieuwe mogelijkheden van het Internet waarbij men zich op meerdere plekken tegelijkertijd kan bevinden, iets was eerder niet mogelijk was. We kunnen deze problemen met betrekking tot regulering respectievelijk niet afdoen met totale anarchie of oude, niet toepasbare, wetgevingen. Maar ook Lessig zijn oplossing doet afbreuk aan de mediumspecificiteit van het Internet, het bouwt grenzen in een netwerk dat juist zijn kracht ontleent aan het ontbreken van deze grenzen. Wat blijft er dan nog over aan mogelijkheden tot regulering van informationele privacy online? We kunnen ons heil zoeken in een vorm van 'collectieve wetgeving', er moet op zoek worden gegaan naar een convergentie van politieke machten die op dezelfde gebieden betrekking hebben als het Internet: overall. Een goede start hierin is genomen door 'overall' te beginnen in Europa en de Verenigde Staten.

In "Regulating Privacy: Data Protection and Public Policy in Europe and the United States" schrijft Colin Bennett (1997) dat met het EU Data Protection Directive (EUDPD) en de Amerikaanse variant (richtlijnen opgesteld door de Federal Trade Commission) een stap in de goede richting is gezet bij de regulering van databescherming en hiermee informationele privacy waarmee uiteindelijk de basis is gezet voor een convergentie in privacy policies, ieder land buiten de EU zou hierbij kunnen aansluiten. Helaas is hier nog niet de oplossing mee gevonden, het probleem dat hier nog wel in speelt is niet politiek, technologisch of economisch maar meer op conceptueel vlak. De EUDPD streeft namelijk naar een "high and common level of protection" (idem : 118). Maar wat wordt precies bedoeld met een dergelijk high level? Hoe wordt deze gewaarborgd? En hoe kan bij alle landen waar dit wordt nagestreefd het succes ervan gemeten worden? Het zijn geen metingen zoals dat gebeurt bij milieubescherming: "[A]ny attempt to establish evaluative criteria for assessing performance is fraught with the central difficulty that the goals of data protection are not self-defining. More holistic perspective is needed that sees data protection as a process that involves a wide network of actors (data users, data subjects and regulators)" (idem : 119-120).

Ons nieuw gevonden probleem betreft dus gebrek aan convergentie door onduidelijke definities binnen de wetgeving. Want hoe kun je iets nastreven als je het niet eens duidelijk kunt benoemen? Eenheid in het consequent en consistent naleven ervan is dus het logische gevolg. Het Internet gaat gewoon door, en bij gebrek aan concrete beschrijvende criteria in de richtlijnen van de EU, of die van de Verenigde Staten, stapte de industrie over op hun eigen oplossing; een oplossing die nog veel meer onduidelijkheid verschafte en allesbehalve een oplossing bleek: de privacy policy.

2.5 policy labyrint en zegels sparen

“Algemene voorwaarden”, “Terms of Use”, “Disclaimer”, “Terms of Service” en tot slot “Privacy Policy”; voor de gemiddelde Internetgebruiker bekende termen. Vraag ze de belangrijkste punten uit een van deze documenten van hun favoriete website op te noemen en toch vallen ze stil. Het is ook niet verwonderlijk; als we alleen al kijken naar de Privacy Policy van Facebook dan telt deze bijna 6.000 woorden. Met een gemiddeld aantal woorden van 2.500 en een gemiddelde leestijd van tien minuten zijn privacy policies een drempel te noemen voor de Internetgebruiker die zich wil registreren voor welke website/dienst dan ook, een drempel die te makkelijk wordt genegeerd.

Maar niet alleen qua hoeveelheid tekst zijn ze een drempel. Deze privacy policies zijn "among the most incomprehensible legal texts around" (Lessig, 2006 : 226). Deze moeilijkheidsgraad van de geschreven teksten in combinatie met de lengte ervan zorgt ervoor dat alleen een heel klein percentage van de bezoekers deze daadwerkelijk leest, en een nog kleiner percentage deze ook daadwerkelijk begrijpt (McDonald en Granor, 2009). Er heerst zelfs onder bezoekers de aanname dat wanneer de website die ze gebruiken een privacy policy heeft, hun persoonlijke informatie veilig is en niet gedeeld zou worden (Hoofnagle et al., 2010). In extreme gevallen zorgt het ontwerp en uiterlijk van een website eerder voor vertrouwen dan het hebben van een privacy policy (Fogg et al., 2002).

Toch grijpt meer dan driekwart van de websites op het Internet naar dit middel om hun 'eigen' beleid uiteen te zetten en zich hiermee in te dekken (idem). 'Eigen' omdat ze in zekere zin nog wel moeten voldoen aan de wetgeving geldend voor het land waarin ze hun bedrijfsactiviteiten voeren. Dit labyrint aan policies is de schuld van het pre-Internet denken over het omgaan met een probleem voor dergelijke duidelijke globale richtlijnen (Lessig, 2006 : 226). De industrie besloot daarom over te gaan op deze afzonderlijke chaos aan privacy policies.

Kijkend naar de actuele praktijkvoorbeelden van problemen met privacy policies komt er nog een derde bovendien: flexibiliteit, ze zijn op elk moment aanpasbaar. De negatieve gevolgen van deze dynamische privacy policies kwamen vooral aan het licht toen Facebook in december 2009 zijn privacy policy veranderde. Deze nieuwe policy hield onder andere in dat bepaalde informatie die eerst door privacy-instellingen als privé ingesteld kon worden nu niet meer instelbaar was en standaard openbaar beschikbaar. Dit had bijvoorbeeld gevolgen voor de lijst van vrienden van de Facebook gebruiker, deze was, ongeacht of deze eerst als privé was ingesteld, opeens voor iedereen (en daarmee het hele Internet) zichtbaar zonder enige optie om dit terug te draaien. 'Facebook's Great Betrayal' (Tate, 2009) werd het genoemd:

Its new privacy policy have turned the social network inside out: millions of people have signed up because Facebook offers a sense of safety. For the last five years — as long as you're relatively careful about who you accept as your friends — what you do and say on Facebook for the most part stays on Facebook ... But virtually overnight and without a clear warning, Facebook has completely reversed those user expectations. Their new privacy

settings amount to making anything you post on Facebook to be public, unless you go to great lengths to keep your info private (Tate, 2009)

Een privacy policy is allesbehalve een zekerheid dat er zorgvuldig met persoonlijke informatie om wordt gegaan. De gecompliceerde teksten, die voor iedere website verschillend zijn en ook nog eens gaandeweg veranderd kunnen worden zijn dus geen vruchtbare oplossing. Wat blijft er dan nog over?

Een andere poging tot zelfregulering vanuit de industrie die op het eerste gezicht iets meer duidelijkheid kan verschaffen in het landschap van privacy policies zijn de zogenaamde online certificaten of "seals of approval". Deze houden in dat de partij die een dergelijk zegel 'draagt' zich aan bepaalde 'Fair Information Practices' omtrent informatiele privacy houdt die opgesteld zijn door de instantie die deze zegels uitgeeft. Enkele voorbeelden zijn TRUSTe, eTrust en Webtrust. Hoewel deze zegels van goedkeuring van een instantie zorgden voor een betere perceptie van de site bij de consument (Miyazaki en Krishnamurty, 2005) zorgt het ook voor een verplaatsing van het probleem. Naast inconsistentie bij het toekennen van deze zegels en het niet effectief reguleren van websites die het zegel al dragen (idem : 44) is er geen partij die het alleenrecht heeft om zegels toe te kennen met een duidelijk statement wat betreft informatiele privacy. In plaats daarvan zijn er talloze commerciële instanties die hun zegel overal op willen plakken, vaak voor een gezonde financiële compensatie (idem).

Deze chaos van policies en zegels die meer onduidelijkheid dan duidelijkheid verschaffen is net als de problemen voor de politieke regulering en wetgeving een reden te meer om te zoeken naar een convergentie van de regulering, maar ook een transparantie in deze. Niet alleen zou dit voor de consument en politiek duidelijker maken waar en hoe informatiele privacy beschermd wordt, ook voor bedrijven wordt op die manier duidelijk aan welke concrete regels ze zich moeten houden en wat er met de data gedaan kan worden.

2.6 de politieke problemen

Bij het determineren van gangbare mogelijkheden voor de regulering van informatiele privacy stuiten we dus op enkele problemen: [1] De voortdurende belangenstrijd tussen overheid, commerciële sector en de consument bij het opslaan, verwerken en toegang hebben tot persoonlijke informatie zorgt voor een moeizame totstandkoming van daadwerkelijke regulering op alle mogelijke vlakken (wetgeving, markt, normen en architectuur). [2] De dynamische ontwikkelingen in het landschap van informatietechnologie en daarmee ook informatiele privacy zorgen voor een constant achterhaalde vorming van wetgeving of wanneer deze uiteindelijk kan worden ingevoerd. [3] Het Internet kent geen eenzijdige globale oplossing voor het jurisdictie probleem; grenzen op het Internet zijn onduidelijk en pogingen tot het opstellen tot collectieve richtlijnen met betrekking tot de flow van persoonlijke informatie worden geremd door het ontbreken van een duidelijke consensus over de concepten die in deze richtlijnen worden gebruikt. [4] Oplossingen die door de industrie zelf worden

geïmplementeerd zoals privacy policies zijn gecompliceerd, inconsistent en hebben praktisch geen autoriteit.

Als we kijken naar deze vier problemen heeft het politieke kader dus vooral problemen doordat het concept en de regulering zich in een constante flux bevinden. Dit is een wisselwerking, zonder duidelijke conceptualisatie van het privacy-probleem is het moeilijk te reguleren. Zonder consistente regulering lijkt het in de praktijk een anarchie waardoor we ons in een vicieuze cirkel bevinden waarbij we alleen maar meer controle over onze privacy verliezen. Convergentie van onder andere wetgeving en een daardoor ook meer transparante regelgeving zijn mogelijkheden die een groot deel van de genoemde problemen uit de weg gaan. Alvorens we nog verder gaan kijken hoe we uit de vicieuze cirkel van controleverlies kunnen breken, zijn er nog twee andere kaders die hun eigen bijdrage aan de erosie van privacy leveren.

privacy & personen

Nu we het eerste probleemgebied hebben behandeld zien we dat het verlies van controle in dit kader vooral komt door gebrek aan regulering door conceptuele onduidelijkheid en het ontbreken van convergentie op het gebied van wettelijke richtlijnen. De gevolgen zijn oplossingen vanuit de industrie die meer kwaad dan goed doen. Maar waar staat de consument in dit geval? Waar staat het individu die de oorzaak is van dit hele debat? Het is immers zijn/haar informatie die op het spel staat. Treft hen blaam? Gedeeltelijk, dit hoofdstuk toont aan waarom de schuld deels bij het individu te leggen is maar werpt ook licht op de kromme machtsrelatie in informationele privacy, een goed dat toch eerst echt alleen van het individu was.

3.1 euro's, dollars en info's

Sociale netwerksites (SNS) kunnen nogal verschillen op de manier waarop ze worden gebruikt: LinkedIn wordt vooral gebruikt voor zakelijke relaties, Match.com als datingsite en Facebook voor een scala aan sociale relaties. Maar ze vertonen ook overeenkomsten, zo maken ze online interactie tussen mensen mogelijk en varen ze allemaal bij de persoonlijke informatie van hun gebruikers. SNS ontlenen hun bestaansrecht en succes vooral aan het mogelijk maken tot delen van informatie. Om de SNS zo volledig mogelijk te gebruiken, wordt er door haar gebruikers een grote en alsmaar groeiende hoeveelheid persoonlijke informatie achter gelaten (Acquisti en Gross, 2006; boyd, 2007).

Minder dan bij deze SNS is, voor de gebruiker, de persoonlijke informatie bij de E-commerce sector op het Internet van belang, want ook op dit platform heeft de consument weinig bezwaar:

Paradoxically, the high level of consumer privacy concern appears to have had little discernible impact on consumers' shopping behaviors. Most consumers are willing to give up some of their privacy to participate in a consumer society. [M]any people would be upset if they were denied the marketing and credit opportunities made available through the use of personal information (Phelps et al., 2000 : 27)

Er gaat bij deze vorm van 'voordeel' voor de consument een zekere vorm van hypocrisie uit. Als consumenten kunnen kiezen tussen privacy of een ander goed/voordeel dan kiezen zij toch snel voor het laatste: gesponsorde credit cards, klanten-kaarten en zoekmachines. Mensen kiezen deze omdat ze gemak bieden, een snellere doorstroom van zaken, financiële voordelen en connectiviteit. Het probleem hierbij is dat mensen niet écht kiezen; ze zijn namelijk niet helemaal op de hoogte van welke zaken ze eigenlijk opgeven bij een zoekopdracht op een zoekmachine of het achterlaten van persoonlijke gegevens bij het meedoen van een online prijsvraag. Hierdoor kunnen ze niet een totaal afgewogen rationele beslissing maken en kiezen ze vaak ongemerkt niet voor privacy.

Voor de gemiddelde winkelier op het Internet kunnen zijn klanten niet genoeg persoonlijke informatie achterlaten. Analyse van koopgedrag en het doen van suggesties op basis hiervan is een

succesvol bewezen manier om de consument te binden en tot nieuwe aankopen te verleiden (Fan et al, 2008). Wat we hier kunnen zien is een tendens in de richting van het gebruik van persoonlijke informatie als een soort betaalmiddel. De consument geeft persoonlijke informatie op in ruil voor het gebruiken van een service. Naast de euro en de dollar lijkt ook persoonlijke informatie een geldige valuta te worden.

Zoals in het begin van deze paragraaf gesteld zijn de beweegredenen voor het delen van informatie bij SNS niet alleen te zoeken in het kunnen gebruiken ervan; het actief meedoen en invulling geven aan het eigen sociale netwerk door het verstrekken van informatie speelt ook een grote rol. Waarom geven wij al deze persoonlijke informatie zo makkelijk af zonder direct te weten wat ermee mag en kan gebeuren? Waarom willen wij ons zo graag 'zichtbaar' maken online? Om tot een antwoord op deze vragen te komen en de problemen hierdoor nog meer naar de oppervlakte te brengen kijken we allereerst naar het werk van socioloog Erving Goffman om vervolgens een parallel te trekken met de huidige identiteitsvorming online.

3.2 the presentation of self in everyday [Facebook] life

In het dagelijkse leven dient ons lichaam als een voorstelling van onze identiteit. Een voorstelling die in deze context een performance behelst. Erving Goffman beschrijft in zijn boek *The Presentation of Self in Everyday Life* (1959) *impression management*: hoe we informatie over onszelf presenteren aan anderen door ons lichaam te gebruiken. Impression management maakt deel uit van een groter proces waarin mensen zoeken naar het definiëren van een situatie op grond van hun gedrag. Mensen zoeken deze definiëring door te kijken naar aanwijzingen uit de context van de situatie. Sociale normen komen hieruit voort en men 'presenteert' zichzelf aan de hand van voor die situatie geschikt gedrag.

Maar hoe lossen we het vormen van de presentatie van onszelf op via een virtueel kanaal als het Internet? Dat doen we door het delen van allerlei mogelijke informatie die bijdraagt aan het construeren van een 'bestaan', een persoonlijke identiteit, op een deel van het Internet, zij het Facebook, LinkedIn of een persoonlijk blog. We schrijven onszelf "into being" volgens Jenny Sundén (Sundén in boyd, 2007 : 12). Maar niet alleen het schrijven is relevant voor het vormen van onze identiteit op de online 'podia'. Het plaatsen van foto's en video's dragen bij aan het ontwikkelen van een virtuele aanwezigheid. Kijkend naar het door Anthony Giddens genoemde "reflexivity of the self" dat nodig is voor identiteitsvorming (Giddens, 1991) zouden we kunnen stellen dat het meedoen aan quizzen op Facebook als "What Greek god are you" of de "Which facebook quiz are you quiz" hier aan bij kan dragen, maar daarmee ook aan een vergaande disseminatie van de rest van hun persoonlijke informatie (Lee, 2009). De keuze van welke persoonlijke informatie wel en niet 'gepost' wordt door mensen op sites zoals Facebook is dus ook toe te schrijven aan de genoemde zelfreflectie in het kader van Bentham's panopticon, alleen zijn het in dit geval de vrienden op het netwerk die mogelijk

meekijken naar je profiel. Want ook de mensen die meekijken zijn verantwoordelijk voor de meerwaarde die participatie aan SNS ons geeft.

Sociale media onderzoeker Danah Boyd ziet deze tendens in het beschikbaar maken van persoonlijke informatie; de drang om sociale interactie tussen vrienden in de publieke sfeer te brengen zodat anderen dit kunnen zien: “Friends are publicly articulated, profiles are publicly viewed, and comments are publicly visible” (boyd, 2007 : 7). Het is niet alleen zo dat anderen dit kunnen zien, derden binnen het sociale netwerk kunnen er ook in meedoen, door erop te reageren, waardoor het ook een mate van sociale betrokkenheid stimuleert. Daarnaast zegt Boyd over MySpace: “many considered participation on the key social network site, MySpace, essential to being seen as cool at school” (idem : 1). Volgens Boyd is deelname aan SNS: “[a] more general desire to be validated by one’s peers. Even though teens theoretically have the ability to behave differently online, the social hierarchies that regulate “coolness” offline are also present online. For example, it’s cool to have Friends on MySpace but if you have too many Friends, you are seen as a MySpace whore.” (idem : 13)

Hoewel in de context van de jongere generatie de term “coolness” duidelijk is, kan het voor een groter publiek (dat actief is op SNS sites) worden vervangen door het eerdergenoemde tonen van sociale betrokkenheid doordat het in wezen een nieuw sociaal netwerk is met een deel van de eigenschappen die het offline ook zou hebben. Het zou gezien kunnen worden als een mix van participatiedrang, narcisme, angst en identiteitsvorming.

Een belangrijke pijler van de voortdurende drang om te participeren in SNS door persoonlijke informatie op de verschillende sites te plaatsen en te delen met een bepaald netwerk aan gebruikers is vooral identiteitsvorming. De reikwijdte van dit netwerk kan in sommige gevallen zelf worden bepaald door bijvoorbeeld de mogelijkheid van privacy-instellingen of het al dan niet accepteren van nieuwe vrienden. Via een SNS is de definitie van ‘een vriend’ niet altijd even duidelijk (Knitel, 2008) maar bij de commerciële sector is helemaal geen sprake van vrienden, noch is daar sprake van identiteitsvorming. Toch laten gebruikers ook daar hun persoonlijke informatie achter; er is ook wel degelijk sprake van een relatie tussen consument en industrie (het zijn alleen geen echte vrienden). Hoe zitten deze relaties precies in elkaar? Waar zijn ze op gebaseerd? En welke problemen kleven hieraan? In de volgende paragraaf zal deze relatie worden geschetst en de privacy-problemen die daarmee opspelen voor ons onderzoek.

3.3 relaties & vertrouwen

“Een relatie opbouwen met de klant” is een logische manier om meer klantenbinding te bereiken en wanneer mogelijk ook meer te verkopen aan diezelfde klant. Het concept van klantenbinding is zeker niet nieuw maar heeft wel nieuwe mogelijkheden gekregen door ontwikkelingen in informatietechnologie. Niet alleen zijn de manieren waarop deze binding bewerkstelligd kan worden uitgebreid (Bauer, 2002), ook de manieren waarop deze omgezet kan worden in resultaat. Zo kan er

flexibiliteit in het productieproces behaald worden door direct inzicht in kooppatronen maar ook gericht worden geadverteerd naar klanten toe (Samarajiva, 1997: 283). Om tot deze mate van inzicht te komen moet er dus sprake zijn van een zekere relatie tussen klant en bedrijf. Deze relaties zijn vaak asymmetrisch.

De asymmetrie in de relatie zit hem in de hoeveelheid informatie die beide partijen van elkaar bezitten en de manier waarop deze wordt verkregen. De individuele consument betreedt de markt voor persoonsgegevens “niet als een gelijke partner van de alliantie van het grootwinkelbedrijf, providers, direct marketers en data-miners” (Van den Hoven, 2002 : 53). Een bedrijf kan via de informatie die bij een transactie mee wordt gestuurd allerlei persoonlijke informatie over de klant automatisch verkrijgen. Terwijl anderzijds de klant, wanneer deze informatie over het bedrijf wil, ernaar moet zoeken op de website en meer gelimiteerd is in de hoeveelheid informatievoorziening van het bedrijf. Deze relatie is op dat moment ‘fragiel’ en het is daardoor belangrijk voor het bedrijf om vertrouwen van de klant te winnen.

Aan vertrouwen moet gewerkt worden; zodra de consument minder vertrouwen krijgt in een bedrijf door bijvoorbeeld ondoorzichtige informatie verzameling en data-mining technieken zou dat tot een vicieuze cirkel kunnen leiden; hoe minder vertrouwen in een service, hoe minder informatie de gebruiker zelf zal geven en hoe meer de service zal grijpen naar andere middelen om hoe dan ook alsnog deze informatie te verkrijgen, wat op zijn beurt weer tot gevolg kan hebben in een negatief effect op de vertrouwensrelatie.

In de praktijk kunnen we deze vicieuze cirkel zien bij Facebook. Een voorbeeld is de introductie van de “News Feed” op Facebook in september 2006. De News Feed is in feite een manier om meer informatie zichtbaar te maken in het netwerk maar ging ten koste van het vertrouwen van haar gebruikers. De informatie die een gebruiker te zien kreeg voor de News Feed lag teveel op de achtergrond of was moeilijk te navigeren. Facebook besloot dit op te lossen door alle informatie en activiteiten van de mensen uit het netwerk van de gebruiker te verzamelen en overzichtelijk in een “feed” weer te geven. Deze verandering bracht een storm aan kritiek met zich mee, vooral omdat gebruikers ineens direct werden geconfronteerd met de informatie die beschikbaar komt door hun activiteiten op Facebook zonder dat ze daar van tevoren duidelijk van op de hoogte waren. Mark Zuckerberg, CEO van Facebook, betoogde na de heftige stroom kritieken dat de veranderingen niets anders waren dan het beter organiseren van de beschikbare informatie. Gevolg was dat velen op Facebook hun privacy-instellingen veranderden en dat er steeds minder informatie in de feed verscheen, het liefst wilde een groot gedeelte van de gebruikers zich ‘uitschrijven’ voor deze News Feed, wat ook te zien is in de 740,000 leden die de Facebook groep “Students Against Facebook News Feed” telde (Arrington, 2006).

Facebook antwoordde met uitgebreidere privacy-instellingen maar laaide het vuur van kritiek weer op door twee jaar later in 2008 te besluiten de News Feed uit te breiden met het toevoegen van posts afkomstig van de Wall van een gebruiker. Alsof dat nog niet genoeg was besloot het in december 2009 de privacy-instellingen die het mogelijk maakten om de News Feed te controleren te

verwijderen. Berichten over de 'evilness of Facebook' vonden door deze nieuwe controverse hun weg op het web. Ook plannen als 'Quit Facebook Day' zagen het licht, een dag waarop men werd aangespoord het Facebook profiel te verwijderen door het aanhoudende schenden van vertrouwen door Facebook van hun gebruikers. Dat laatste werd uiteindelijk geen groot succes maar geeft wel aan dat het schaden van een vertrouwensrelatie met de gebruikers gevolgen kan hebben voor de toegang tot informatie van die persoon, namelijk niks meer.

Er liggen dus zeker interpersoonlijke relatie-eigenschappen ten grondslag aan een relatie die niet tussen natuurlijke personen is. Meer dan alleen vertrouwen: "privacy is not just one possible means among others to insure some other value, but that it is necessarily related to ends and relations of the most fundamental sort: respect, love, friendship and trust. Privacy is not merely a good technique for furthering these fundamental relations; rather without privacy they are simply inconceivable" (Fried, 1968 : 477). Nu is er in het geval van bijvoorbeeld Facebook niet helemaal sprake van een vriendschap of zelfs een vorm van liefde tussen het platform en haar gebruikers, maar een mate van respect zouden veel gebruikers toch wel op hun plek vinden: "Facebook's new default privacy settings are the biggest, longest, proudest middle finger a site's ever given me" aldus Chris Sacca (2010) op zijn Twitter na de invoering van de nieuwe privacy-instellingen.

Privacy-instellingen impliceren dat ze een mogelijkheid tot controle met zich meedragen; een vorm van informatie vrijgeven of beperken in een mate die de instellingen representeren. Beperking van de outflow van persoonlijke informatie is een belangrijk gereedschap in het behouden en terugwinnen van privacy-controle. In de volgende paragraaf zullen de voornaamste beweegredenen tot beperking worden besproken die daarmee ook aanstippen waarom juist in beperking een van de belangrijkste oplossingen voor het terugkeren van een controle over privacy besloten ligt.

3.4 voorkomen van schade, binnen alle contexten

Privacy-instellingen zouden, als we Jeroen van den Hoven moeten geloven, eigenlijk "damage control" moeten heten: "Als persoonsgegevens makkelijk toegankelijk zouden zijn dan zou de kans op misbruik daarvan tot directe schade van de betrokken persoon aanzienlijk toenemen. [...] We willen de kans op schade [...] verkleinen. Dat heeft niets met privacy te maken, maar primair met het voorkomen van schade" (Van den Hoven, 2002 : 53). Van den Hoven heeft het over vier verschillende morele redenen om de toegang tot persoonsgegevens te beperken. Naast het voorkomen van schade voor een individu doordat persoonlijke gegevens in de openbaarheid komen, komt ook de eerder beschreven asymmetrische relatie terug; Van den Hoven noemt dit "het nastreven van fairness en het realiseren van complexe informatiegelijkheid" (idem : 54): "The information marketplace is far from level, with insufficient protections in place to ensure that exchanges are governed by 'openness, transparency, participation, and notification on the part of business firms and direct marketers to secure fair contracts'" (Van den Hoven, 2004 : 435).

Daarnaast noemt hij het probleem van de integriteit van informatiesferen, door Walzer (1984) de “separate spheres of justice” genoemd. Deze (maatschappelijke) contexten hebben ieder hun eigen ongeschreven morele regels voor de allocatie van toegang tot informatie en persoonsgegevens. Zo mogen we ervan uitgaan dat de medische sfeer gescheiden is van de commerciële sfeer en de dokter niet informatie van zijn patiënten op de markt te gelde maakt. Deze maatschappelijke contexten zijn van belang als we willen spreken over het verliezen van controle over privacy. Men is namelijk niet altijd boos als hun persoonlijke informatie in sommige contexten beschikbaar is, mensen begrijpen namelijk dat dit cruciaal is voor een sociaal leven (Nissenbaum, 2009). Het probleem zit hem in de “inappropriate, improper sharing of information” (idem : 240); iets wat door het Internet op steeds grotere schaal voorkomt. Deze contexten worden daardoor alleen nog maar onduidelijker, ze verstoren de algemeen geaccepteerde flows van informatie; ze overschrijden normen. Het is daarom van belang dat we opnieuw kijken naar onze normen in bepaalde contexten en daarnaar handelen. De zorgen om privacy moeten niet alleen gecentreerd zijn rondom het controleren van persoonlijke informatie maar rondom de informatie die nodig is in een bepaalde context en daar moet niet van af geweken worden. Hoewel we naar een zekere vorm van transparantie zoeken, is het niet de transparantie in onze persoonlijke leven die door het overschrijden van deze contexten tot stand komt zoeken. De integriteit van contexten, informatiesferen, moet behouden worden, ook op het Internet, hoe moeilijk ook.

Als laatste noemt Van den Hoven nog de morele autonomie die gevaar loopt als constant “de blik, het oordeel en de inmenging van anderen [daarmee] interfereren” (Van den Hoven, 2002 : 54). Dit pleidooi voor een controle over dat wat anderen tot oordelen en de vorming van meningen en beelden over ons aanzet is te herleiden tot de activiteit die centraal staat in dit onderzoek: het controleren van de privacy. In het geval van SNS is dit eigenlijk een probleem dat men over zichzelf afroept door te participeren in het netwerk. Het is een onontkoombaar probleem dat bij iedere participatie die tot stand komt door het brengen van persoonlijke informatie vanuit de privé sfeer naar een publieke context speelt.

“Een publieke context”, want is er iets eenzijdigs zoals een ‘publieke context’ of een ‘publiek’? Craig Calhoun (1992) heeft in *Habermas and the Public Sphere* dit debat al uitgebreid gevoerd over wat ‘publiek’ nu eigenlijk inhoudt. Met het Internet wordt dit concept nog complexer. De dichotomie publiek en privé is niet alleen door de verschillende contexten niet meer zo duidelijk te stellen, ook door de mogelijkheden die bijvoorbeeld SNS bieden om je eigen context te creëren binnen het publiek. Voordat we daarop ingaan, laten we eerst nog eens kijken naar de problemen van een dergelijke dichotomie voor ons onderzoeksterrein.

3.5 publiek en privé

Een dichotomie heeft vaak een negatieve connotatie en dat is ook niet gek want het tekent twee concepten lijnrecht tegen elkaar af zonder dat de grenzen vaak zo duidelijk zijn als ze doen

vermoeden. Zo ook bij de dichotomie tussen publiek en privé. Vooral wanneer deze dichotomie op het Internet wordt gelegd; in hoeverre is er dan nog sprake van iets privé? “Alles wat op het Internet gebeurt is toch publiekelijk?” is een veelgehoord argument (boyd, 2007 : 16). Voordat we te doen hadden met de digitale media was het duidelijk wanneer er sprake was van een van de twee domeinen (Nissenbaum, 2009 : 94). “A man’s home is his castle” en dat was daarmee gelijk zijn privé-sfeer. Dit was tot de opkomst van de nieuwe media een breed aangenomen notie (idem).

Maar waar kunnen we nog een privé-plek vinden op het Internet? Danah Boyd merkt op dat jongeren zelf op zoek gaan naar hun privé-plekjes op Internet, niet geheel toevallig het een “my space in a networked public” noemend:

When teens argue for having my space in a networked public, they are trying to resolve the social problems that emerge because the constructions of public and private are different online and off. In unmediated spaces, structural boundaries are assessed to determine who is in the audience and who is not. The decision to goof off during lunch is often made with the assumption that only peers bear witness. In mediated spaces, there are no structures to limit the audience; search collapses all virtual walls. (danah boyd, 2007 : 16)

Maar we kunnen het zoeken naar privé-plekken op Internet verder trekken naar het eerdergenoemde idee van contexten. De notie dat het Internet publiek zou zijn is waar tot op een zekere hoogte. Het betekent namelijk niet dat alle informatie die erop geplaatst wordt direct ook publiek is. Men kan, ook op het Internet, zijn eigen kasteel bouwen, alleen of met een groep andere gebruikers. Want iets wat privé is in het ene kasteel, of context, kan publiekelijk toegankelijk zijn in het andere. Het is op basis van deze dat we context-relatieve informatie-normen opstellen (Nissenbaum, 2009 : 141). Er wordt teveel tijd verspild aan het beslissen of een gedeelte van onze informatie privé of publiek is terwijl we eigenlijk juist willen kijken welke beperkingen we willen opleggen aan de flow van informatie in verschillende contexten.

We kunnen, als we bijvoorbeeld kijken naar een gedeelte persoonlijke informatie in de vorm van vakantiefoto’s al stellen dat deze in de ene context op het web wél worden gedeeld en de andere niet. Niet alleen kun je die contexten zien in de verschillende platformen zoals Facebook en LinkedIn, waarbij de laatstgenoemde niét de juiste plaats is voor deze foto’s, ook binnen de sites zelf kan soms een eigen context worden gecreëerd. Op Facebook is het perfect mogelijk dat je een fotoalbum met vakantiefoto’s wel met de bewuste vrienden die mee waren wilt delen maar niet met de collega’s van het werk. Het feit dat een site als Facebook op deze manier inspeelt op het hebben van verschillende groepen ‘vrienden’ en dus ook verschillende context-relatieve informatie-normen is een duidelijk gegeven dat privé op het Internet veelzijdiger is dan alleen ‘niet beschikbaar voor het publiek’.

3.6 problemen op het sociale vlak

Wanneer we teruggaan naar het begin van dit hoofdstuk en nog even op een rij zetten welke problemen we nu zijn tegengekomen zowel in de literatuur als in de praktijk kunnen we de volgende

problemen distilleren: [1] mensen zien vaak niet de problemen van het afgeven van persoonlijke informatie voor het gebruik van een service, privacy wordt hierdoor impliciet gezien als een betaalmiddel in plaats van een kwetsbaar en kostbaar goed. [2] Het delen van persoonlijke informatie is een belangrijke eigenschap van identiteitsvorming, ook op het Internet. Hierdoor is er een soort tweestrijd gaande tussen het wel of niet gebruiken van een sociaal netwerk en het deelnemen in de informatiestroom van deze. [3] De asymmetrische relaties die gebruikers/consumenten hebben met de bedrijven waarmee informatie wordt uitgewisseld zijn vooral een gevolg van de ontbrekende transparantie van deze bedrijven en de mate waarop de mogelijkheden tot informatiewinning over het individu steeds verder ontwikkeld worden. De neerwaartse spiraal waarin vooral vertrouwen en respect een grote rol spelen wordt door afbreuk hiervan bij het ontbreken van transparantie alsmaar langer. Het voorkomen van schade op basis van de disseminatie van persoonlijke informatie wordt onder andere op deze manier bemoeilijkt. [4] Het Internet zorgt voor een vervaging van grenzen in informatiesferen, het doet afbreuk aan de integriteit van deze en daardoor wordt het moeilijker om grip te hebben op de flow van informatie binnen deze contexten.

Nu we ook deze problemen hebben blootgelegd zijn de oplossingen voor deze vooral te vinden in beperking en transparantie. Transparantie om duidelijkheid te hebben in de gevolgen van het afgeven van persoonlijke informatie voor het gebruiken van een service; een transparantie in de flow van jouw persoonlijke informatie. In welke informatiesferen wordt het gebruikt? Wie kunnen het zien? Wat wordt er mee gedaan en wat heeft het voor gevolgen voor mijn privacy? Alvorens we overgaan tot concrete mogelijkheden in oplossingen is het belangrijk nog één veld mee te nemen in het distilleren van de problemen rondom controle van privacy online, het veld dat in de eerste plaats platform biedt voor de erosie van privacy.

technologie

We zijn nog steeds op zoek naar de verantwoordelijke problemen voor het verliezen van de controle over individuele privacy online. *Online* en dus: het Internet. Dat Internet dat zoveel deuren heeft geopend voor de privacy erosie waar we nu mee te maken hebben. In de voorgaande twee hoofdstukken hebben we kunnen zien welke problemen het Internet daar teweeg brengt. Welke problemen liggen in de verantwoordelijke informatietechnologie zelf besloten voor het verliezen van de controle over privacy en kunnen we daar verbeteringen in tegemoet zien? Wellicht met het gebruik van diezelfde technologie? Dit hoofdstuk bewandelt de weg daar naar toe.

4.1 de ubiquitous paradox

De innovatie op het gebied van informatietechnologie lijkt geen rem te kennen; sneller, kleiner en verbonden zijn sleutelwoorden in deze. Het verschijnsel waarbij verbonden computers langzaam opgaan in de omgeving op een onopvallende manier wordt naar gerefereerd als *ubiquitous computing* (Bellotti, 1997). Ubiquitous computing kan ingezet worden voor datadiensten die op de achtergrond plaatsvinden. Het is ironisch te noemen dat de bijna onzichtbare verwerking van verbonden computers in onze dagelijkse omgeving bijdraagt aan een *zichtbare* erosie van onze privacy; vooral wanneer gebruikers niet eens in de gaten hebben wanneer ze 'online' zijn of onbewust onderhevig zijn aan dataverzameling.

FourSquare, een dienst voor de mobiele telefoon, maakt het mogelijk voor mensen om op elk moment van de dag online in te checken op een locatie waar ze zich op dat moment offline bevinden. Zo wordt er een bericht gestuurd naar FourSquare dat men incheckt op het centraal station Utrecht wanneer men zich ook daadwerkelijk daar bevindt. "Technology applied without context will behave obnoxiously, and smart devices will make people do stupid things" aldus Malcom McCullough (2006 : 27), dat hij gelijk heeft kunnen we ook zien in het FourSquare voorbeeld. De gevolgen van zulke locatie-gebaseerde software voor informationele privacy kan zo ver reiken als inbraak en stalking (Ringelstijn, 2010). Sites als *pleaserobme.com* proberen, door expliciet de mensen weer te geven die melden dat ze op vakantie gaan, of via FourSquare laten zien dat ze in ieder geval van huis gaan, bewustwording te creëren voor deze gevolgen.

Als we nog even terugkomen op het citaat van McCullough: "... smart devices will make people do stupid things" (McCullough, 2006 : 27) kan dat meerdere zaken impliceren. Bijvoorbeeld dat het systeem slimmer is dan de gebruiker, omdat het impliceert dat het deze stomme dingen laat doen. Of de gebruiker kent het ingewikkelde systeem niet goed genoeg en doet er daardoor verkeerde of stomme dingen door. Ongeacht de interpretatie van dit citaat, ontbreekt dus een mate van kennis voor correcte omgang met de gebruikte media. De gebruiker moet hiervoor een zekere vorm van media

literacy (Potter, 2005) bezitten of het systeem moet in een dergelijke mate transparant genoeg zijn om de werking ervan te kunnen communiceren met de gebruiker.

Niet alleen tijdens of na het gebruik, maar zeker ook ervoor zoals Bellotti (1997) beschrijft in twee case studies van media-spaces. Deze ruimtes kwamen tot stand door het gebruik van audio- en videoverbindingen tussen verschillende kantoren. Het grootste probleem zegt Bellotti is de vorm van *disembodiment* en *dissociation* die dergelijke ubiquitous computing omgevingen met zich meebrengen (idem : 69). Men is ineens zichtbaar voor een andere omgeving zonder dat het individu hier zelf fysiek kan zijn of bewust kan communiceren met de mensen die zich daar bevinden.

De flow van persoonlijke informatie wordt hiermee deels overgeleverd aan het systeem, het verlies van controle over deze is wederom een probleem. Maar het is belangrijker om de gebruiker te laten weten dat hij/zij in de gaten gehouden kan worden; op dat moment kan er in ieder geval voor worden gekozen om zich niet in die ruimte te bevinden of de media niet te gebruiken. Er kan dan, door het individu, een afgewogen keuze gemaakt worden en de juiste acties toegekend aan het vrijgeven van deze informatie. Door feedback gebrek ontstaat dus een controle gebrek en hiermee juist geen gebrek aan de beschikbaarheid van persoonlijke informatie.

4.2 jaren bewaren

Geen gebrek dus aan persoonlijke informatie, maar waar laat je al die informatie? En wat doe je ermee? "The point and the advantage of the technology is that information is gathered as a resource, and the purpose of the data cannot be specified until it is used, if at all, at some unpredictable time in the future" (Bellotti, 1997 : 93). Het maakt niet uit, "pakken wat je pakken kan" lijkt het motto bij de huidige trend van dataverzameling. Content is key, content is king, of concreter in deze context: persoonlijke informatie is kostbaar voor bedrijven. Het kan gebruikt worden om bijvoorbeeld invulling en betekenis te geven aan een sociaal netwerk of voor het omzetten van deze informatie in 'kennis'. Kennis in nieuwe inzichten voor bijvoorbeeld het consumentengebruik van een service te krijgen en hierop in te spelen. Door kennis over een klant en zijn/haar transacties of zoekopdrachten kunnen bijvoorbeeld persoonlijke aanbiedingen worden gedaan, zoeksuggesties of aanpassingen aan het productieproces plaatsvinden.

Met het opslaan van deze flows aan informatie spelen enkele problemen op. Hoe sla je deze namelijk op? Wie heeft er toegang tot deze opslag? Waar wordt het opgeslagen? En hoe lang moet de data beschikbaar blijven? Viktor Mayer Schönberger gaat in *Delete: The Virtue of Forgetting in the Digital Age* (2009) in op deze problemen die opspelen bij de eindeloze drang naar het opslaan van data, waardoor al onze digitale transacties permanent een spoor van informatie achterlaten, ook als er nog geen directe bestemming voor beschikbaar is.

Mayer-Schönberger beschrijft hoe informatiemanagement bij de mens sinds het begin der tijden voornamelijk was om te vergeten, omdat het onthouden van gebeurtenissen kwam met hoge inherente kosten. taal en de 'externe harde schijven van vroeger' (vertelde verhalen, papier) speelden

een veel grotere rol bij het onthouden en vergeten, zij hebben de basis gelegd voor de huidige maatschappij. Met de steeds lagere kosten voor het opslaan van informatie op het digitale geheugen is het effectiever om informatie opgeslagen te houden dan deze achteraf te verwijderen. Dit heeft zowel voor- als nadelen, maar de negatieve implicaties zijn hier logischerwijs het probleem.

Met de komst van deze digitale archieven en zekere eindeloze opslag wordt de waarde van het vergeten van zaken vooral voor het individu groter. Het verleden van een individu en de controle daarover door deze is een belangrijk heikel punt geworden door de permanente digitale sporen die we achterlaten op het Internet. De mogelijkheden in het doen vergeten, of dus het verwijderen, zijn de pijlers van controle over de eigen persoonlijke informatie voor een individu; alleen op deze manier is het mogelijk een "social forgiveness" te bewerkstelligen en hiermee het eigen heden te bepalen (Smith, 2010 : 372).

Weke gevolgen heeft het jaren bewaren van informatie in de praktijk voor informationele privacy? Mayer-Schönberger noemt de volgende twee praktijkvoorbeelden: allereerst de zaak waarbij een vrouw werd geweigerd voor het verkrijgen van een onderwijs certificaat doordat zij op MySpace te vinden was met een foto getiteld "Drunken Pirate". De vrouw klaagde de desbetreffende school vervolgens aan maar had hier geen succes mee. Vervolgens het verhaal van een psychotherapeut die toegang tot de Verenigde Staten werd geweigerd omdat een douanebeambte via Google een 30 jaar oud paper had gevonden van de man waarin hij toegeeft LSD te hebben gebruikt (Mayer-Schönberger, 2009 : 11-14).

In 2007 zei zoekmachine Google dat het tot dan toe iedere zoekopdracht die ooit ingegeven was door een gebruiker en de links die ze daarna aan klikten in de resultaten had opgeslagen. Door het georganiseerd opslaan van alle gebruikte zoekwoorden, ongeveer meer dan 30 miljard per maand (idem : 14) is het mogelijk om inzicht te krijgen in bijvoorbeeld demografische zoekrends. Maar belangrijker is de mogelijkheid om de meta-informatie van deze zoekopdrachten te gebruiken om deze te verbinden aan een individu, om zo een compleet profiel te kunnen optekenen uit alle informatie die bekend is over deze. Gecombineerd met het gebruik van andere Google diensten door dit individu is de hoeveelheid persoonlijke informatie waar Google toegang tot heeft alsmaar groeiende, en die kan niet zomaar worden vergeten, of wel?

"Google knows [...] details we have long forgotten, discarded from our mind as irrelevant, but which nevertheless shed light on our past: perhaps that we once searched for an employment attorney when we considered legal action against a former employer, researched a mental health issue, looked for a steamy novel, or booked ourselves into a secluded motel room to meet a date while still in another relationship" (idem : 14)

Bijna letterlijk kan Google meer over ons onthouden dan wijzelf, maar, zo heeft Google in 2008 laten weten om het vertrouwen van haar gebruikers niet kwijt te raken: niet voor altijd. Google gaf aan dat het in het vervolg na negen maanden de data zal anonimiseren; een deel van de veelomvattende persoonlijke informatie zal dan worden vergeten. Een stap in de goede richting voor de houdbaarheid

van onze persoonlijke informatie bij Google. Het verkleint het risico op onbedoelde of onvoorzien gebruik van deze informatie. Maar dat geeft ons er nog geen individuele controle over: geen mogelijkheid om met een druk op de knop Google het te doen vergeten.

Het ontbreken van beperking komt dus ook aan de oppervlakte bij problemen op technologisch vlak voor privacy. Een beperking in de hoeveelheid dataverzameling en de periode dat de persoonlijke informatie beschikbaar blijft zal de mate waarin privacy-controle verloren raakt drastisch verminderen. In de volgende paragraaf wordt duidelijk dat het beperken van toegang ook gereedschap is voor controle.

4.3 toegang en beveiliging

Persoonlijke informatie is te vergelijken met een soort kluis, een aantal kluisen; het is alleen toegankelijk als men er de sleutel toe heeft. Die sleutel dragen wij als individu zelf en eventuele kopieën van die sleutel geven wij af aan mensen die we vertrouwen. Soms geven we alleen de sleutel van een bepaalde kluis, de kluis met bijvoorbeeld onze NAW gegevens, of een gedeelte daarvan. Andere keren mogen anderen ook de sleutel tot je vakantiealbum. Met de komst van het Internet krijgen we het ineens druk met het uitdelen van sleutels: een paar voor Google, een doosje vol voor Facebook, LinkedIn krijgt het Curriculum Vitae sleuteltje en zo verliezen we langzaam maar zeker het zicht en de controle over onze uitgedeelde sleutels. Het grootste probleem hiermee is, als je een sleutel kwijt bent kun je niet meer zomaar de sloten veranderen.

Het bepalen wie of wat toegang heeft tot welke informatie en in welke mate wordt, zoals we in het eerste hoofdstuk zagen, als de fundering voor een dergelijke definitie van privacy gezien (o.a. Gavison, 1980; Westin, 1967). Charles Fried (1968) zoekt de definitie meer in de term controle over informatie dan in toegang tot informatie. Maar in de term controle ligt ook controle over toegang besloten. Uiteindelijk komt het op hetzelfde neer: een individu wordt aangetast in zijn/haar informationele privacy wanneer derden er toegang tot hebben zonder dat het individu directe controle heeft over deze toegang.

Een duidelijk voorbeeld van de problemen die opspelen bij het verliezen van controle over de toegang tot- is te zien in een praktijkvoorbeeld van Facebook en haar partners. Op Facebook zijn mensen verbonden met de mensen die ze kennen, met publieke figuren en diensten en producten waar ze 'fan' van zijn. In april 2010 presenteerde Facebook het zogenoemde "Open Graph". Een platform dat toegang biedt tot al deze informatie aan andere websites en applicaties. Als je bijvoorbeeld via je Facebook gebruikersnaam en wachtwoord inlogt bij Yelp, krijgt Yelp toegang tot onder andere je woonplaats, favoriete eten en muziek (mits je dit in je profiel hebt aangegeven) en kan het op basis daarvan suggesties doen. Het eerdere Facebook Connect bood deze functionaliteit ook aan maar Open Graph maakt het mogelijk voor de deelnemers om data van hun gebruikers voor langer dan 24 uur op te slaan op hun eigen servers. Facebook introduceerde ook de 'Like' button, die

overal op een website van derden geplaatst kan worden, klik je op deze knop als je bent ingelogd, dan wordt de website naar je profiel op Facebook gepost.

Met Open Graph introduceert Facebook voor haar partners een kopietje van de sleutelbos die je in de eerste instantie als gebruiker alleen aan Facebook af had gegeven. Natuurlijk moet je wel eerst de andere service, zoals Yelp, autoriseren alvorens ze toegang hebben tot deze informatie. Het probleem alleen is dat er aan de ene kant een laagdrempelige manier wordt gecreëerd om andere sites te gaan gebruiken: het is niet meer nodig bij elke site al je registratiegegevens weer in te moeten vullen. Aan de andere kant is het onduidelijk voor de gemiddelde gebruiker welke gevolgen dit heeft. "Open Graph" zal de gemiddelde bezoeker weinig zeggen; wederom is het de transparantie in de gevolgen van het delen van persoonlijke informatie die mist voor de gebruiker.

Wat met de informatie vervolgens gebeurt, is een ding, hoe de informatie beveiligd wordt is weer een hele andere zaak. Een zaak waar Yelp, tot op heden, zich al twee keer in heeft vergist. Door fouten in de programmering van Yelp was het mogelijk om op de achtergrond data van andere gebruikers te verzamelen; data die alleen beschikbaar zou zijn voor Yelp werd op deze manier blootgesteld aan iedereen die het wilde. De beveiliging van dergelijke systemen is terecht een groot heikel punt bij vele privacy voorvechters. Want zoals in de vorige paragraaf al aangegeven brengt het opslaan van persoonlijke informatie de nodige complicaties met zich mee. Naast de probleemvelden tijd (hoe lang wordt de data opgeslagen) en macht (wie kan het controleren) is nu ook de beveiliging te noemen. Maar hoe weet je als gebruiker of de te gebruiken dienst de beveiliging goed op orde heeft? Het is de zoveelste oproep voor transparantie om een beter inzicht in de flow van persoonlijke informatie te krijgen en daarmee controle.

4.4 overal en altijd

Nu we ook het laatste probleemveld voor privacy hebben geanalyseerd kunnen we de volgende problemen hieruit opmaken. [1] Door de toenemende vorm van ubiquitous computing waarbij verbonden media op steeds meer mogelijke manieren worden ingezet en de toenemende complexiteit van deze computers is het voor het individu moeilijk om te bepalen waar, wanneer en hoe er een outflow van zijn/haar persoonlijke informatie plaatsvindt. Het gebrek aan transparantie, feedback en kennis van het systeem vormen hierbij de oorzaken. [2] Het opslaan van data wordt steeds goedkoper en eenvoudiger en de manieren waarop data geanalyseerd en gebruikt kunnen worden steeds uitgebreider en lucratiever. Dit heeft tot gevolg dat veel instanties grote hoeveelheden aan persoonlijke informatie van hun gebruikers tot hun beschikking hebben en houden. De wijdverspreidheid en de ondoorzichtige wijze in het opslaan van deze informatie maken het vrijwel onmogelijk voor het individu om hier controle over uit te oefenen. [3] Door het afgeven van persoonlijke informatie aan een instantie, betekent dat nog niet dat alleen die instantie daar beschikking over heeft. Afspraken van het bedrijf met andere partners en de ontwikkeling van platformen zoals Open Graph kunnen ervoor zorgen dat deze informatie wordt doorgespeeld. [4]

Beveiliging van technologie die informatie-uitwisseling mogelijk maakt is complex en het individu heeft hier weinig tot geen inzicht in of controle over. Men is afhankelijk van een correcte en veilige dataopslag van de provider.

De grootste problemen die technologie met zich meebrengt voor het controleren van informationele privacy zitten dus vooral in het feit dat dataverzameling en opslag onbeperkt, ondoorzichtig, overal en altijd plaats kan vinden. Nu we de problemen op alle drie de probleemgebieden hebben blootgelegd wordt het tijd om te gaan kijken naar de mogelijkheden voor het oplossen van het verliezen van controle over onze privacy. *Het oplossen van het oplossen van controle.*

controle

Nu alle drie de velden zijn behandeld waar problemen aangewezen kunnen worden in het verlies van controle over privacy is het vervolgens zaak om de mogelijkheden op het gebied van het terugkrijgen van deze controle te bekijken. Het is belangrijk om hierbij niet alleen in te gaan op de probleemanalyse en oplossingen van ieder afzonderlijk vlak, maar ook mogelijkheden te presenteren in een hybride van deze. Kijkend naar de probleemanalyses kunnen de oplossingen voor het terugwinnen van controle over privacy gedistilleerd worden tot enkele kernbegrippen in de vorm van *beperking*, *convergentie*, *transparantie* en *(er)kennis*. Deze kernbegrippen hangen nauw met elkaar samen en in enkele gevallen zijn ze aanvullingen op elkaar. In dit hoofdstuk behandel ik ieder begrip en de oplossingen die deze inhouden.

5.1 beperking

Het lijkt een simpele oplossing: als je de controle over je privacy niet wilt verliezen: houd de persoonlijke informatie dan voor jezelf of beperk deze tot een minimum. Zoals aangetoond in de probleemanalyses is het delen van persoonlijke informatie een onderdeel van identiteitsvorming, sociale relaties of het gebruik maken van andere voordelen, het is daarom niet zo eenvoudig om zomaar deze outflow van persoonlijke informatie te stoppen. In de loop van dit hoofdstuk wordt duidelijk dat sommige van de drie andere gebieden van oplossingen; convergentie, transparantie en (er)kennis, ook een beperking van deze flow tot gevolg kunnen hebben. In deze paragraaf zullen meer directe manieren om deze flow te beperken tot het noodzakelijke worden genoemd; dit kan gerealiseerd worden door beide zijden van de informatiestroom: vanuit individu en industrie.

Allereerst kijken we naar de mogelijkheden voor het individu. De eerste oplossing die kan bijdragen door middel van beperking is te vinden in de technologie, want technologie is niet alleen de vijand als het gaat om het verliezen van controle. Het kan juist ook bijdragen aan het terugwinnen hiervan, bijvoorbeeld door Privacy Enhancing Technologies (PET). Privacy voorvechters kunnen hierdoor volgens Agre niet meer technologie louter als schuldige aanwijzen maar ook als middel tegen disseminatie van persoonlijke informatie:

By applying advanced mathematics to the protection of privacy, they disrupt the conventional pessimistic association between technology and social control. No longer are privacy advocates in the position of resisting technology as such, and no longer can objectives of social control be hidden beneath the mask of technical necessity. As a result, policy debates have been opened were many had assumed that none would exist, the simple tradeoff between privacy and functionality has given way to a more complex tradeoff among potentially numerous combinations of architecture and policy choices. (Agre, 1997 : 5)

PET zijn er in verschillende soorten; ze kunnen helpen om de outflow van persoonlijke informatie te anonimiseren en te controleren. In het eerste geval zijn het programma's die alle meta-informatie die men meestuurt op het Internet kunnen anonimiseren. De andere variant maakt het mogelijk om informatiestromen te versleutelen en alleen andere personen die toegang mogen hebben tot deze informatie in een code te voorzien om de informatie te kunnen ontcijferen (o.a. Mannan en van Oorschot, 2008; Lessig, 2006). Voor gebruik op sociale netwerksites hebben deze PET niet erg veel nut omdat de gebruiker ervan nog steeds voorziet in het verspreiden van zijn/haar informatie om waarde te geven aan het sociale netwerk. Belangrijk om aan te stippen is dat deze gereedschappen er niet zijn om alle outflow tegen te gaan maar deze in ieder geval tot een minimum te beperken. Het is alleen zaak deze PET kenbaar te maken bij het grote publiek en uitleg te geven over de manier waarop het gebruikt kan worden.

Maar ook voor de sociale netwerksites zijn er technologische initiatieven om de beperking ook daar te realiseren en toch een gesloten sociaal netwerk te hebben wat paradoxaal genoeg een "distributed open source social network" heet: Diaspora: "They conceive of it as the "privacy aware, personally controlled, do-it-all distributed open source social network," one on which people share strictly on their own terms. Every user will have their own encrypted, customizable "node" on the Diaspora network, and personal data will reside on that user's computer, as opposed to a centralized hub." (VanHemert, 2010).

Niet alleen laat Diaspora je een eigen gecontroleerd sociaal netwerk opzetten maar laat het je deze ook invullen door de data die bij andere instanties is weggezet terug te halen: "reclaim your data" (idem). Een wenselijke toevoeging zou zijn als het vervolgens deze data dan ook, voor zover mogelijk, verwijderd bij de andere partij. Want niet alleen de outflow van informatie moet beperkt worden, ook de houdbaarheid van deze.

Het probleem van de houdbaarheid van informatie en het gebrek aan controle hierover is moeilijk te reguleren. Als we zoeken naar oplossingen moeten deze vooral gezocht worden in politieke regulering. Er kunnen dan twee verplichtingen worden toegevoegd aan de genoemde EU Data Protection Directive: [1] Instanties die persoonlijke informatie van een individu bezitten moeten de mogelijkheid bieden deze ten alle tijde door het individu te kunnen laten verwijderen/aan te passen. [2] Er moet een wettelijk bepaalde maximale periode van houdbaarheid zijn voor verzamelde persoonlijke informatie, bij het verstrijken van deze periode na de verzameling moet de data worden verwijderd of geanonimiseerd worden zodat deze niet meer te herleiden is tot een te identificeren individu. Beide verplichtingen worden respectievelijk in ieder geval nageleefd door grote spelers op de markt zoals Facebook en Google. Facebook heeft het mogelijk gemaakt het profiel te kunnen verwijderen. Eerst moest dit nog door een mail te sturen naar het bedrijf, tegenwoordig kent Facebook toch een "Delete Button". Google heeft aangegeven zoekdata na negen maanden te anonimiseren (Helft, 2008).

Dan is er ook nog een laatste oplossing te noemen in de strijd voor het beperken van het verliezen van controle over privacy en die ligt in het creëren van een soort van fictieve privacy. Gloria

Fuster (2009) ziet een nieuwe Privacy Enhancing *Tool* in plaats van Technology in de vorm van onnauwkeurigheid. Fuster noemt “misrepresentation, partial truths, or the creation of ‘clouds of inaccuracy’” (idem : 89) als manieren om het individu te beschermen tegen disseminatie van hun persoonlijke informatie. Door het beperken van het achterlaten van echte informatie kan bijvoorbeeld wel van een dienst gebruik worden gemaakt zonder dat daar concessies aan verlies van privacy voor plaatsvinden. Onnauwkeurigheid in informatie kan helaas niet altijd worden ingezet als middel omdat het soms meer complicaties dan voordelen op kan leveren (idem : 29) maar wanneer het mogelijk is, en deze situaties moeten door later genoemde (er)kennis ontwikkeling worden herkend, dan is het zeker een gereedschap om toe te voegen aan de derde interpretatie van de T in PET: de Privacy Enhancing Toolbox.

5.2 convergentie

Als we nogmaals kijken naar de grootste knelpunten op politiek vlak voor privacy, is het duidelijk dat we hiervoor oplossingen moeten zoeken in jurisdictionele convergentie en actualiteit en compleetheid met aanvulling van sociale normen en technologische hulpmiddelen. Want beperking kan ook op deze vlakken plaatsvinden.

Over internationale privacy wetten is al vaak gesproken (o.a. Ritter et al, 2001; Shaffer, 2000) maar een vruchtbare uitkomst is er tot op de dag van vandaag nog niet concreet. Het meest werkbaar voorstel komt van een niet expliciete privacy-voorvechter: Jeffrey Palmer schrijft in zijn voorstel voor een internationale milieuwet (1992) wat we zoeken voor internationale privacywetgeving. Hij stelt een aantal belangrijke speerpunten op waar deze internationale milieuwet aan moet voldoen (idem : 281). Veel van deze punten zijn bepalingen in het naleven van de regels en sancties die noodzakelijk zijn voor een werkbaar aanpak. Een selectie andere regels zijn, in het licht van conceptualisatie en (er) kennis, ook van toepassing op een mogelijk voorstel voor internationale wetgeving voor privacy en databescherming:

A Director-General and staff [...] to have explicit international responsibilities for educating people about the global environmental problems and what they can do to help. [...] A thorough preparatory process, in which there are ample notice, thorough scientific and technical preparation, and consultation before regulations are made. [...] Formal provision for authoritative and widely representative scientific advice and papers to be available to the organization. (idem)

Een instantie aanstellen met de verantwoordelijkheid voor het wijzen op de gevaren voor privacy van het Internet helpt mee aan het bereiken van een zekere kennis op dit vlak die idealiter zich uit in correct handelingsvermogen. Uitgebreid advies van experts op het gebied van privacy en technologieën en de hedendaagse (en toekomstige) gevaren zijn nodig voor conceptueel begrip en kennis van de technologische gevaren en uitdagingen voor de instantie die de richtlijnen en wetten opstelt; een dergelijke collectieve wettelijke aanpak valt of staat namelijk alleen maar bij een duidelijke

conceptualisatie van het object en de actoren die hierin meespelen. Alleen de snelheid waarmee deze conceptualisatie en actoren kunnen veranderen in het huidige informatietijdperk vragen nog voor een andere eigenschap van de richtlijnen.

De anticipatie op nieuwe technologieën en hun mogelijk (nadelige) invloed op informationele privacy moet zo snel mogelijk kunnen plaats vinden in een dergelijke nieuwe wetgeving. Flexibiliteit en snelle doorvoering door een autoritaire convergentie zijn daarom deel van de fundering van een allesomvattend en effectief pakket aan wetgeving.

Kijkend naar de huidige stand van zaken zou het EU Data Protection Directive de meeste potentie hebben om tot een werkbare internationale privacy-wet te komen. Potentie, want de fundering voor deze richtlijnen zijn in 1995 al opgesteld, ruim voor de echte opkomst van het Internet, en daarmee alle problemen rondom informationele privacy bij dit medium.

Naast het conceptuele en 'kennis van'-probleem dat opgelost kan worden door het voorstel van Palmer hiervoor te lenen moet er ook duidelijk worden gemaakt waar de macht ligt in deze regulering; een eigen implementatie door iedere afzonderlijke lidstaat, zoals nu, is geen werkbaar plan. Dit zou een stap terug in de convergentie betekenen. Voor een eenzijdige aanpak moet een centraal orgaan, dit kan ook in de vorm van een samenwerking, aangewezen worden die hiermee niet alleen op papier belast wordt, maar ook in de praktijk. Belangrijk is om een dergelijke regelgeving en regulerende instantie niet te zien als een totalitaire privacy waakhond maar als een hulpmiddel voor alle overheden om met een complex probleem als privacy om te gaan: "the argument here is not for some utopian system of world government. It is merely for a limited extension of the existing institutions of international law so that the law can cope effectively with a new problem. The proposal does require nations to surrender some sovereignty. It is palpably in their self-interest to do so" (Palmer, 1992 : 283).

Met duidelijke internationale regelgeving kunnen we ook het probleem van privacy policies uit de weg gaan. Privacy policies mogen dan op geen enkele wijze rechtsgeldig zijn wanneer zij afwijken van de globale wetgeving. Op het gebied van zogenaamde privacy seals zou, in samenwerking met het voorgestelde centraal orgaan voor privacywetgeving, een algemeen certificaat worden uitgegeven waarmee een instantie laat zien te voldoen aan de internationale eisen voor privacy. Dit certificaat moet zowel bij het centrale orgaan als bij de instantie gevalideerd kunnen worden door de gebruiker op een eenvoudige manier.

Voor bovenstaande wetgeving worden vooral de nodige stappen gevraagd van overheid en de bedrijfssector. De consument kan voornamelijk in de volgende paragraaf zelf bepalen in hoeverre hij/zij controle over privacy verliest, behoudt of wint.

5.3 transparantie

"Wat gebeurt er met mijn persoonlijke informatie als ik op deze knop druk?", het antwoord op een vraag als deze moet eigenlijk al direct door het gebruikte systeem gegeven worden, of het antwoord

moet al bekend zijn bij de persoon. De manier waarop dit bereikt kan worden is door transparantie en feedback van het systeem, alleen op een dergelijke manier kan een gebruiker genoeg kennis vergaren om te weten wat de gevolgen zijn voor het activeren van een flow aan persoonlijke informatie.

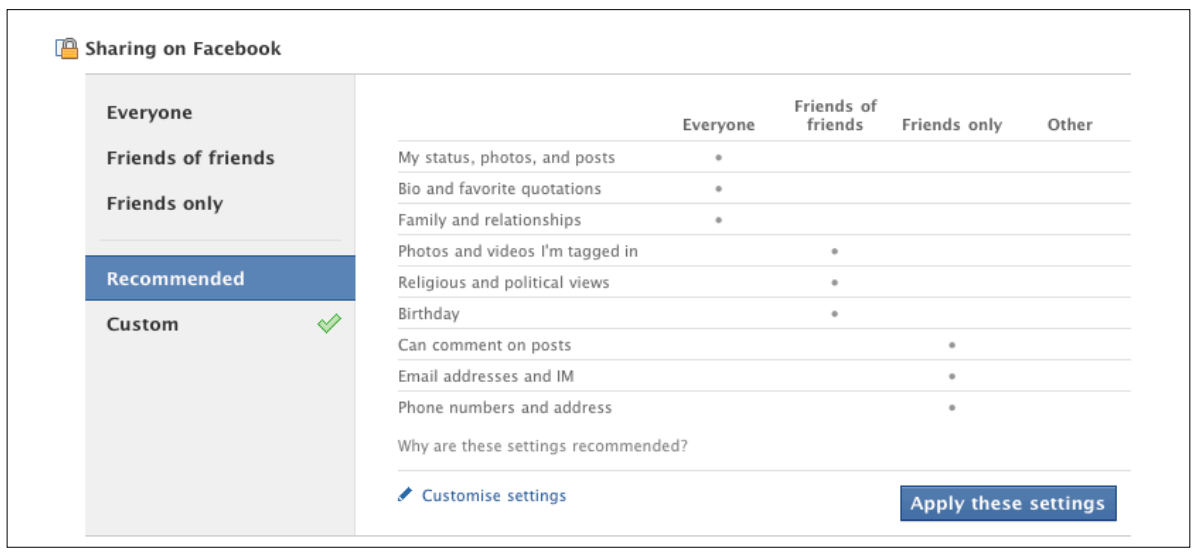
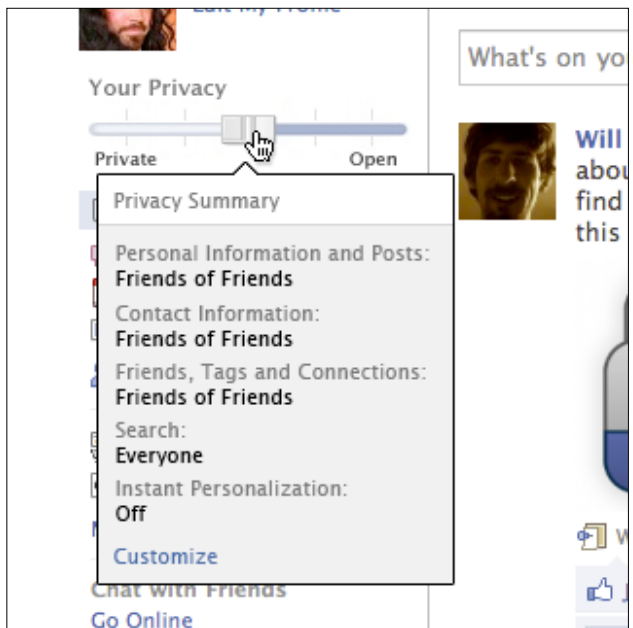
Door een gebruiker te laten weten welke gevolgen een activiteit zoals het gebruik van een web-dienst of het zich bevinden in een fysieke media-ruimte (Bellotti, 1997) of het identificeren, taggen, van vrienden en zichzelf op een foto op Facebook kan hebben, kan het zich bewust worden van de privacy die diegene op dat moment bezit en wat de status van die privacy is na de activiteit. Deze transparantie kan op verschillende niveaus behaald worden; concreet vertaalt zich dat naar de volgende oplossingen voor bijvoorbeeld het Facebook platform.

Transparantie in interface design: Facebook is al vaak beschuldigd van het hebben van onduidelijke privacy-instellingen. Vele iteraties zijn er al aan vooraf gegaan (Cordova, 2010) en ook de huidige generatie 'privacy settings' kunnen nog veel beter en prominenter⁴ voor de gebruiker aanwezig zijn (Bilton, 2010). Zo vonden ook de oprichters van *YourOpenBook.org*.

YourOpenBook.org creëert met haar website in de eerste instantie bewustwording door een overzicht te geven van publiekelijk zichtbare status updates van Facebook gebruikers met sleutelwoorden als bijvoorbeeld "cheated" en "new pics". Vervolgens stellen de makers ook de volgende Interface verandering (afbeelding 2a) voor op het gebied van een 'privacy control'. In plaats van de privacy-instellingen weg te werken op een aparte pagina onder Instellingen zoals Facebook doet (afbeelding 2b) beslaat hun voorstel een controle element dat ten alle tijden zichtbaar is op iedere pagina. Ook is er voor gekozen deze instellingen intuïtiever te maken waarbij directe feedback te zien is bij het verschuiven van de slider, de gevolgen voor het aanpassen van deze standaard settings bij iedere waarde staan ook direct aangegeven onderaan; door de mate van privacy te visualiseren wordt het voor de gebruiker transparanter welke mate van privacy zij aan hun flow van informatie toekennen.

⁴ Of zelfs in de moedertaal van de gebruiker. Facebook biedt een genationaliseerde interface aan, maar voor de privacy-instellingen was dit niet het geval; deze waren louter in het Engels beschikbaar (Wang, 2010)

afbeelding 2a: voorgestelde meer transparante privacy-controle van YourOpenBook.org



afbeelding 2b: privacy-instellingen op Facebook

Ook is de standaard instelling volledig naar links geschoven wat een profiel dat alleen zichtbaar is voor vrienden inhoudt. Dit is in tegenstelling tot de standaard, aanbevolen, instellingen van Facebook (afbeelding 2b) waarbij de status updates, foto's, posts, familie en vrienden voor het hele Internet beschikbaar is.

Toch zijn deze privacy-instellingen vergeleken bij die van 2009 (Cordova, 2010) een stap in de goede richting, maar alleen als je er effectief naar zoekt. Om de gebruiker tegemoet te komen in dat zoeken en bewustwording te creëren van de bestaande flow van persoonlijke informatie op het netwerk biedt *ReclaimPrivacy.org* een te gebruiken plugin voor de browser die bij activering de gebruiker waarschuwt voor de huidige- en helpt bij het herstellen van de privacy-instellingen tot een - voor de gebruiker- gewenst niveau. Maar deze aanpassing gebeurt pas achteraf, zou het niet beter zijn de gebruiker van tevoren al te waarschuwen voor het publiek dat toegang krijgt tot de te delen informatie?

Een vink zetten naast “Ik ga akkoord met de Algemene Voorwaarden” of een dergelijke zin; het moet vrijwel bij elke dienst op het web. Met de genoemde collectieve wetgeving zou een groot gedeelte van deze voorwaarden, op het gebied van informationele privacy, in ieder geval strakgetrokken en van tevoren kenbaar moeten zijn. Toch zou, in het licht van transparantie, een directe feedback naar de gebruiker op zijn plaats zijn: “Let op, door het gebruiken van deze dienst wordt uw naam, email adres en telefoonnummer opgenomen in ons systeem. We kunnen deze gebruiken om u aanbiedingen te doen via mail of telefoon, wilt u dit niet, klikt u dan op annuleren”. In dit voorbeeld is de mate van feedback beknopt en duidelijk. Het zou utopisch denken zijn om aan te nemen dat ieder bedrijf een dergelijke korte uitleg van het gebruik van persoonlijke informatie zou hebben. Het is daarom zaak om, mede in het licht van de vertrouwensrelatie tussen gebruiker en dienstverlener, de juiste balans te vinden tussen transparantie, zoals informatievoorziening over de gevolgen van het verstrekken van persoonlijke informatie, en het behouden van gebruiksvriendelijkheid.

De gebruiker wordt door dergelijke feedback bewust van de gevolgen voor de flow van zijn/haar persoonlijke informatie. Maar transparantie door informatievoorziening creëert niet automatisch een geïnformeerde samenleving, transparantie is een stap naar een bewuste Internetgebruiker die voor zover mogelijk de controle over zijn/haar privacy in de hand heeft; informeren is namelijk een ding, interpretatie van deze informatie is een tweede. Het informatielandschap dat rondom die transparantie aanwezig is biedt namelijk meer mogelijkheden. Mogelijkheden die ons nog verder tot een geletterde handelingsbekwame persoon op het Internet maken; een persoon die niet alleen weet wat er met zijn privacy gebeurt maar hier ook op kan anticiperen. We hebben beperking, convergentie en nu ook transparantie behandeld, de laatste is in alle drie de oplossingen al genoemd en kan zowel als middel en als doel worden gedefinieerd.

5.4 (er)kennis

Naar de vaardigheid in het consumeren van media wordt vaak gerefereerd als “media literacy”. Een geletterd persoon in de media kan volgens Patricia Aufderheide: “decode, evaluate, analyze and produce both print and electronic media. The fundamental objective of media literacy is critical autonomy in relationship to all media” (Aufderheide, 1997 : 79), en daar zijn we naar op zoek, een

kritisch autonoom individu die weet welke gevolgen media-activiteiten voor zijn/haar privacy hebben en daarop kan anticiperen.

Want de kennis van een deel van de gevolgen is in het geval van Facebook wel bekend (boyd, 2010a), het ontbreekt alleen aan de anticipatie. Het is hypocriet te noemen dat Facebook gebruikers zoveel informatie blijven delen op het platform en tegelijkertijd hun grootste zorgen uitspreken over de gevolgen hiervan (idem). “Quit Facebook Day” was een dag die bedoeld was om hier een einde aan te maken maar uiteindelijk een dag was die aan velen voorbij is gegaan (Howard, 2010). De gebruikers erkennen dus de problemen maar nemen geen effectieve maatregelen. Danah Boyd merkt op dat gebruikers teveel waarde aan Facebook zijn gaan hechten en problemen hebben hier zomaar uit te stappen: “they have invested time, energy, resources, into building Facebook what it is. They don’t trust the service, are concerned about it, and are just hoping the problems will go away [...] we should all be working to help people understand what’s going on” (boyd, 2010b).

Informatie door transparantie is dus een oplossing, interpretatie van deze informatie, het plaatsen van deze informatie in de juiste context en vervolgens adequaat handelen is de benodigde aanvulling op deze oplossing. Een aanvulling die kan worden bereikt door educatie, een noodzakelijke educatie willen we weer de controle over onze privacy krijgen. Deze educatie is net zo hard nodig als de regulering van bovenaf: “Data protection is a learning exercise that involves a mutual process of education and mediation from the bottom up as much as it involves regulatory command from the top down” (Bennett, 1997 : 199).

In *Confronting the challenges of participatory culture: Media education for the 21st century* beschrijft Henry Jenkins (2009) de mogelijkheden om deze educatie te bewerkstelligen in een “participatory culture” waarin iedereen content produceert en consumeert, waaraan toegevoegd moet worden in het kader van privacy dat produceren het consumeren, van deze productie, door anderen tot gevolg heeft. Het is in mijn onderzoek niet de bedoeling deze mogelijkheden allen uiteen te zetten. Wat ik hier wel mee duidelijk wil maken is dat als men het vermogen heeft om informatie te creëren, te delen en te verwerken dan moet het ook het vermogen hebben om dit op een zo bewust mogelijke weloverwogen manier te kunnen doen zonder daarbij de controle erover onbewust weg te geven.

besluit

We begonnen dit onderzoek met de vraag "op welke manieren kunnen verbeteringen worden aangebracht in het controleren en reguleren van individuele privacy online op sociaal, technologisch en politiek vlak?". Door een duidelijk concept te vormen van privacy in het eerste hoofdstuk konden we vervolgens op zoek gaan naar de actuele problemen geschetst in het bestaande wetenschappelijk debat en de weerspiegeling daarvan in de praktijk in de drie hoofdstukken die daarop volgden.

Problemen zijn gevonden in vooral het ontbreken van beperking, convergentie, transparantie en (er)kennis. Uiteindelijk moesten in deze vier begrippen ook de oplossingen worden gezocht. Het gebruik van PET, eenzijdige politieke maatregelen die toereikende jurisdictie hebben, meer transparantie afdwingen bij de verantwoordelijke instanties en bewustwording creëren en daardoor correct handelingsvermogen bij het individu zijn de belangrijkste oplossingen die in het laatste hoofdstuk zijn geschetst. Het is een stap dichterbij de richting van het behouden of terugwinnen van de controle over privacy online. De theoretische basis is gelegd, het volgende probleem is de daadwerkelijke implementatie om dit verlies van controle een halt toe te roepen.

Als metafoor voor het verliezen van controle over privacy en het terugwinnen van deze voor het individu zie ik een goede kandidaat in erosie. Erosie is een slijtageproces van een vast oppervlak waarbij materiaal verplaatst of zelfs geheel verdwijnt. Onze privacy overkomt eenzelfde proces. De flow waarmee de grond bij erosie verschuift is ook te zien in onze persoonlijke informatie. Langzaam maar verplaatst onze persoonlijke informatie van de privé sfeer naar andere informatiesferen. "Plant een boom" is de titel van dit onderzoek en een maatregel om erosie tegen te gaan; begroeiing is nodig om controle te krijgen over de grond die anders onder onze voeten wegglijdt.

Het overgrote deel weet hoe we erosie tegen kunnen gaan, en toch blijven we maar bomen kappen; conflicterende belangen zijn de oorzaak. Onze sociale netwerken online zijn een gevestigd sociaal platform van uiting, onze kortingen op Internet hebben we nodig. Dat er ook andere manieren zijn om tot eenzelfde resultaat te komen, al is dat het planten en kappen van bomen elders, het correct instellen van onze privacy-instellingen, het gebruiken van PET of het opgeven van valse informatie, is vaak bekend maar is meestal niet de makkelijkste of voordeligste weg van handelen.

Alle actoren in de problemen rondom privacy controle online staan bovenaan te kijken naar de langzaam maar verschuivende en afbrokkelende grond bezaaid met persoonlijke informatie. Enkelen staan klaar om het beneden op te vangen. Politiek, industrie, individu en technologie, allen zijn ze een klein beetje verantwoordelijk. De boodschap van dit onderzoek is om de handen ineens te slaan en die bomen te gaan planten, in de eerste instantie afzonderlijk in ons eigen gebied, maar bij elkaar mag natuurlijk ook.

discussie

In dit onderzoek is vooral aandacht geweest voor de positieve waarde van privacy in het algemeen maar voornamelijk op het Internet. De eerder getrokken parellel met copyright voor politieke regulatie kan hier nu ook genoemd worden om de problemen van het streven naar zo'n groot mogelijke privacy op het Internet te onderstrepen. Anonimiteit nodigt uit tot crimineel gedrag (Lessig, 2006 : 225) en het is daarom ook beter om te streven naar een vorm van pseudonimiteit zoals voorgesteld door Lessig waarbij de regulerende instanties nog altijd kunnen ingrijpen en activiteiten op het Internet nog kunnen herleiden naar een individu: "Friends of privacy will be furious with any endorsement of surveillance. But [...] a sophisticated surveillance technology might actually increase effective privacy, if it decreases the instances in which humans intrude on other humans" (idem).

Het was ook niet mijn bedoeling om met dit onderzoek te pleiten voor totale anonimiteit op het Internet, het overheidsaspect heb ik daarom ook bewust achterwege gelaten in dit werk. De problemen die ik heb aangestipt zijn vooral de eenvoudige manieren van dataverzameling die mogelijk zijn gemaakt door het Internet en de instanties die deze data zonder concrete doeleinden verwerken.

De politieke oplossingen in dit onderzoek zijn pure theoretische suggesties die in de praktijk nog geen wijdverspreide adaptatie kennen. De politieke implicaties die opspelen bij een dergelijke collectieve invoering van wetgeving zijn door mij alleen aan de oppervlakte bekeken. In het academisch kader van de mediawetenschappen waar ik mij in bevind reikt dit ook niet tot mijn expliciete kennisgebied.

De door mij voorgestelde oplossingen zijn louter mogelijkheden in de goede richting om controle te behouden en terug te winnen. Praktische implementatie van deze oplossingen op alle genoemde vlakken zijn een plek voor collega's in de gerelateerde academische velden.

literatuur

Acquisti, A., & Gross, R. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In G. Danezis & P. Golle, *Privacy Enhancing Technologies*, Lecture Notes in Computer Science (4258, pp. 36-58). Berlin: Springer.

Agre, P. E., & Rotenberg, M. (1997). *Technology and privacy: the new landscape*. Cambridge: MIT Press.

Arrington, M. (2006). Facebook Users Revolt, Facebook Replies. *TechCrunch*. Via <http://techcrunch.com/2006/09/06/facebook-users-revolt-facebook-replies/> .

Aufderheide, P. (1997). Media Literacy: From a Report of the National Leadership Conference on Media Literacy. In R. Kubey, *Media literacy in the information age: current perspectives*. New Jersey: Transaction Publishers. 79-86.

Bauer, H. (2002). Building customer relations over the Internet. *Industrial Marketing Management*, 31 (2), 155-163.

Bellotti, V. (1997). Design for Privacy in Multimedia Computing and Communications Environments. In P. E. Agre & M. Rotenberg, *Technology and Privacy: The New Landscape* (pp. 63-98). Cambridge: MIT Press.

Bennett, C. (1995). Privacy in the political system: perspectives from political science and economics. In A. Westin, *Privacy and Freedom: updated Social Science Perspectives on Privacy*. New York: Atheneum.

Bennett, C. J. (1997). Convergence Revisited: Toward a Global Policy for the Protection of Personal Data? In P. E. Agre & M. Rotenberg, *Technology and Privacy: The New Landscape* (pp. 99-124). Cambridge: MIT Press.

Berkvens, J., & Prins, C. (2007). *Privacyregulering in theorie en praktijk*. Amsterdam: Kluwer.

boyd, d. (2007). Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life. *MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital*.

boyd, d. (2010). Public by Default, Private when Necessary. Via http://www.zephoria.org/thoughts/archives/2010/01/25/public_by_defau.html.

boyd, d. (2010). Quitting Facebook is pointless; challenging them to do better is not. Via <http://www.zephorias.org/thoughts/archives/2010/05/23/quitting-facebook-is-pointless-challenging-them-to-do-better-is-not.html>

Calhoun, C. (1992). *Habermas and the public sphere*. Cambridge: MIT Press.

Cordova, C. (2010). The End of Privacy as We Know It?: The Ethics of Privacy on Online Social Networks.

Davies, S. G. (1997). Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity. In P. E. Agre & M. Rotenberg, *Technology and Privacy: The New Landscape* (pp. 143-166). Cambridge: MIT Press.

Fan, Y., Shen, Y., & Mai, J. (2008). *Study of the Model of E-commerce Personalized Recommendation System Based on Data Mining*. 2008 International Symposium on Electronic Commerce and Security (pp. 647-651). IEEE.

Flaherty, D. (1988). The Emergence of Surveillance Societies in the Western World: Toward the Year 2000. *Government Information Quarterly*, 5(4), 377-387.

Fogg, B. J., D, P., Soohoo, C., Danielson, D., Marable, L., Stanford, J., et al. (2002). How Do People Evaluate a Web Site's Credibility? Results from a Large Study. *October*.

Fried, C. (1968). Privacy. *Yale Law Journal*, 77(2), 475-483.

Fuster, G. G. (2009). Inaccuracy as a privacy-enhancing tool. *Ethics and Information Technology*, 12(1), 87-95.

Gavison, R. (1980). Privacy and the Limits of Law. *Yale Law Journal*, (89), 421-71.

Giddens, A. (1991). *Modernity and self-identity: self and society in the late modern age*. Palo Alto: Stanford University Press.

Goffman, E. (1959). *The Presentation of Self in Everyday Life*. New York: Anchor Books.

Goldsmith, J., & Wu, T. (2006). *Who Controls the Internet: Illusions of a Borderless World*. New York: Oxford University Press, USA.

Goodwin, C. (1991). Privacy: Recognition of a Consumer Right. *Journal of Public Policy & Marketing*, 10(1), 149-166.

Gutwirth, S. (2009). *Reinventing Data Protection?*. Tilburg: Springer.

- Hixson, R. F. (1987). *Privacy in a Public Society: Human Rights in Conflict*. New York: Oxford University Press, USA.
- Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?* SSRN eLibrary. Working Paper Series.
- Howard, A. B. (2010). On the failure of Quit Facebook Day, Social Utility and Privacy. *digiphile*. Via <http://digiphile.wordpress.com/2010/05/31/on-the-failure-of-quit-facebook-day-social-utility-and-privacy/>.
- Hoven, van den, J. (2002). Wadlopen bij Opkomend Tij, Denken over ethiek en informatiemaatschappij. In J. de Mul, *Filosofie in cyberspace: reflecties op de informatie- en communicatietechnologie* (pp. 49-66). Kampen: Klement.
- Hoven, van den, J. (2004). Privacy and the Varieties of Informational Wrongdoing. In R. A. Spinello & H. T. Tavani, *Readings in Cyber Ethics* (2 ed., p. 430). Sudbury: Jones and Bartlett Publishers.
- Jenkins, H. (2009). *Confronting the challenges of participatory culture: Media education for the 21st century*. Cambridge: MIT Press.
- Johnson, D. R., & Post, D. G. (1996). Law And Borders- The Rise of Law in Cyberspace. *Stanford Law Review*, 48, 1367. SSRN.
- Kincaid, J. (2010). Yelp Security Hole Puts Facebook User Data At Risk, Underscores Problems With 'Instant Personalization'. *TechCrunch*. Via <http://techcrunch.com/2010/05/11/yelp-security-hole-puts-facebook-user-data-at-risk-underscores-problems-with-instant-personalization/>.
- Knitel, J. (2008). "Add as a friend": een onderzoek naar connectors op Facebook. *Universiteit Utrecht*.
- Langheinrich, M. (2001). Privacy by design—principles of privacy-aware ubiquitous systems. *UbiComp 2001: Ubiquitous Computing*, 2201, 273-291.
- Learmonth, M. (2010). Facebook Stirs Up Trouble for Silicon Valley. *Advertising Age*. Via http://adage.com/digital/article?article_id=143646.
- Lee, T. G. (2009). The Startling Truth Behind Facebook Quizzes: What You Don't Know Others Know About You . *21 september, 2009*. Via <http://www.newuniversity.org/2009/09/features/the-startling-truth-behind-facebook-quizzes-what-you-dont-know-others-know-about-you/>.
- Lessig, L. (2006). *Code: version 2.0*. New York: Basic Books.

Mannan, M., & Oorschot, P. V. (2008). Privacy-enhanced sharing of personal content on the web. In *Proceeding of the 17th international conference on World Wide Web*, 487-496. New York: ACM.

Mayer-Schonberger, V. (2009). *Delete: The Virtue of Forgetting in the Digital Age*. Oxfordshire: Princeton University Press.

McCullough, M. (2006). On the Urbanism of Locative Media. *Places*, 18(2), 26-29.

McDonald, A., & Granor, L. (2008). The Cost of Reading Privacy Policies. In *Telecommunications Policy Research Conference*.

Michael, J. (1994). *Privacy and human rights: an international and comparative study, with special reference to developments in information technology*. Boston: Dartmouth Publishing.

Miguel, H. (2008). Google Tightens Data Retention Policy - Again. *New York Times*. Via <http://bits.blogs.nytimes.com/2008/09/09/google-tightens-data-retention-policy-again/>.

Miyazaki, A. D., & Krishnamurthy, S. (2002). Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions. *Journal of Consumer Affairs*, 36(1), 28-49.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79(1), 119-158.

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

Orwell, G. (1949). *Nineteen Eighty-Four. A novel.*. London: Secker & Warburg.

OV Chipkaart. (2010). Privacybeleid. *OV-Chipkaart*. via <http://www.ov-chipkaart.nl/algemeen/onderkant/privacy/>.

Palmer, G. (1992). New Ways to Make International Environmental Law. *The American Journal of International Law*, 86(2), 259-283.

Peters, J. D. (1999). *Speaking into the Air: A History of the Idea of Communication*. Chicago: University Of Chicago Press.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, 19(1), 27-41.

Reiman, J. (1995). Driving to the panopticon: A philosophical exploration of the risks to privacy posed by the highway technology of the future. *Santa Clara Computer and High Technology Law Journal*, 11 (1), 27-44.

Ringleestijn, T. (2010). Gebruikers locatiediensten vrezin inbrekers. *WebWereld*. Via <http://webwereld.nl/nieuws/66584/gebruikers-locatiediensten-vrezin-inbrekers-.html>.

Ritter, J., Hayes, B., & Judy, H. (2001). Emerging trends in international privacy law. *Emory International Law Review*, 15, 87.

Sacca, C. (2010). Twitter / Chris Sacca. *Twitter*. Via <http://twitter.com/sacca/status/13108118466>.

Samarajiva, R. (1997). Interactivity As Though Privacy Mattered. In P. E. Agre & M. Rotenberg, *Technology and Privacy: The New Landscape* (pp. 277-310). Cambridge: MIT Press.

Shaffer, G. (2000). Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of US Data Privacy Standards. *Yale Journal of International Law*, 25, 1–88.

Smith, M. L. (2010). Review: Viktor Mayer-Schönberger, Delete: the virtue of forgetting in the digital age. *Identity in the Information Society*, 2(3), 369-373.

Solove, D. J. (2006). A Taxonomy of Privacy, 154 (3), 477-560. SSRN.

Tate, R. (2009). Facebook's Great Betrayal. *Gawker*. Via <http://gawker.com/5426176/facebooks-great-betrayal>.

VanHemert, K. (2010). Diaspora: The Student-Made, Privacy-Respecting Facebook Alternative. *Gizmodo*. Via <http://gizmodo.com/5537502/diaspora-the-student+made-privacy+respecting-facebook-alternative>.

Walzer, M. (1984). *Spheres Of Justice: A Defense Of Pluralism And Equality*. New York: Basic Books.

Warren, S., & Brandeis, L. (1890). Right to privacy. *Harvard Law Review*, 4(5), 193.

Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum.

Whitaker, R. (1998). *The End of Privacy: How Total Surveillance Is Becoming a Reality*. New York: The New Press.

De twee 'normale' bomen in de illustratie op het voorblad van dit werk is afkomstig van de homepage van Forrst. Via <http://forrst.com>

